Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

# Internet et la protection de la vie privée et des données à caractère personnel

De Terwangne, Cécile

*Published in:*
L'Europe des droits de l'homme à l'heure d'Internet

*Publication date:*
2019

*Document Version*
le PDF de l'éditeur

Link to publication

*Citation for pulished version (HARVARD):*
De Terwangne, C 2019, Internet et la protection de la vie privée et des données à caractère personnel. Dans *L'Europe des droits de l'homme à l'heure d'Internet.* Pratique du droit européen, Larcier , Bruxelles, p. 325-368.

**General rights**
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

**Take down policy**
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. May. 2023

strada lex

# CHAPITRE 9. INTERNET ET LA PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES À CARACTÈRE PERSONNEL

Cécile DE TERWANGNE
Professeur à la Faculté de Droit de l'UNamur
Directrice de recherche au CRIDS (UNamur)

## I. Introduction

### A. – *Internet, zone de tous les dangers pour la vie privée et les données personnelles*

Le développement spectaculaire d'Internet et des multiples services qui y sont associés offre de grandes possibilités et d'indéniables avantages. Le recours aux réseaux de communication, et en particulier à Internet, a permis le déploiement de services inimaginables tout en accroissant l'efficacité et l'accessibilité des services classiques. L'utilisation de ce réseau présente toutefois aussi de nombreux défis, en particulier pour la protection des droits et libertés de chacun. C'est le sort réservé aux données relatives aux individus qui suscite une attention particulière et fait l'objet de la présente contribution. D'autant que la phénoménale valeur économique et sociétale que ces données représentent aujourd'hui dans le monde d'Internet explique qu'elles sont l'objet de convoitises concurrentes et au cœur d'intérêts rivaux.

Derrière l'usage d'Internet, la réalité concernant le sort des données à caractère personnel est préoccupante : données recueillies à l'insu des personnes, données réutilisées pour des finalités inavouées, données conservées des mois voire des années, données transmises à des tiers, données confidentielles diffusées... Les individus faisant usage du réseau et de toute la variété de services en ligne existant désormais perdent dans une grande mesure la maîtrise de leurs données. Ils ne savent pas ce qui en est fait, ils ne peuvent contrôler à distance qui y accède. Une série d'acteurs d'Internet, par contre, connaissent leurs goûts, leurs



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



centres d'intérêt, leurs achats, leurs mouvements, les endroits qu'ils fréquentent et les personnes avec qui ils sont en relation. Contrairement à ce que l'on peut penser de prime abord, en effet, naviguer sur Internet laisse bien davantage de traces que déambuler et agir dans la vie réelle. À l'inverse de ce qui se passe dans le monde physique réel, il n'est pas question de se promener sur les inforoutes, d'entrer dans les magasins virtuels, de lire le journal en ligne, d'être intéressé par une annonce commerciale… sans que cela se sache. Toutes les actions effectuées sur Internet laissent des traces entre les mains de différentes personnes. On ne peut manquer de s'interroger sur cette transparence permanente qui ne serait sans doute pas tolérée dans le monde réel.

Internet permet donc la collecte massive de données personnelles sur les citoyens, les acheteurs en ligne, les utilisateurs de réseaux sociaux, etc. L'utilisation largement répandue d'identifiants (tels l'adresse IP ou un numéro de session dans un cookie) permet de lier un utilisateur à ses actions, sa position géographique ou ses données. Ces informations peuvent être analysées et corrélées pour en déduire d'autres, notamment à des fins de profilage. Les conséquences en sont des risques accrus de fuites d'information et de traçage des personnes, mettant ainsi à mal la vie privée de celles-ci[1].

Cette perte de contrôle est d'autant plus inquiétante qu'elle s'accompagne de l'*eternity effect*. À l'inverse de la mémoire humaine, la mémoire électronique n'efface rien si ce n'est volontairement. Au vu de la puissance des moteurs de recherche, tant qu'on n'a pas pris la décision, le temps et l'énergie de les supprimer, des éléments peuvent remonter éternellement du passé. Le passé devient « omni-présent ».

À cela s'ajoutent la fascinante mais aussi effrayante caisse de résonnance universelle qu'Internet offre aux propos et images diffusés et la capacité d'expression publique qui est désormais offerte non seulement aux médias traditionnels mais également à tout un chacun. Ce formidable renforcement de la liberté d'expression peut aussi conduire à des actes malveillants. Ainsi, diffuser une information diffamatoire ou confidentielle sur Facebook, poster une vidéo intime ou humiliante sur YouTube, ou créer un faux article sur quelqu'un dans Wikipédia peut causer des dommages d'une ampleur sans précédent dans la vie *off-line*.

1 J.-N. COLIN, C. DE TERWANGNE, « Protection de la vie privée et des données personnelles dans l'environnement numérique », in *Vie privée et données à caractère personnel* (C. DE TERWANGNE éd.), Bruxelles, Politeia, 2013, 19 p.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



Cette réalité met sérieusement en cause le droit au respect de la vie privée ainsi que le droit à la protection des données.

### B. – *Des textes juridiques européens révisés pour répondre adéquatement aux dangers*

Sur le continent européen, législateurs et juges sont intervenus pour apporter une réponse aux défis suscités pour la vie privée et la protection des données par le déploiement d'Internet. Des textes majeurs viennent d'être adoptés, renouvelant des textes originels dépassés par les développements techniques et sociétaux. Ils proviennent du creuset européen mais ont indéniablement vocation à porter leurs effets bien au-delà des frontières européennes[2]. C'est particulièrement vrai pour la Convention 108 modernisée (dite aussi « Convention 108+ ») du Conseil de l'Europe, adoptée le 18 mai 2018, qui est ouverte à la signature de tous les États du monde[3]. Le texte initial datant de 1981 avait déjà recueilli ces dernières années l'adhésion de six États non européens[4] au-delà de celle acquise des 47 États du Conseil de l'Europe. Mais le Règlement général sur la protection des données (RGPD)[5], norme de l'Union européenne venue remplacer la directive 95/46 et entrée en

2 Voy. sur ce point la contribution de Claire Gayrel dans le présent ouvrage.

3 Le texte initial, la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, a fait l'objet d'un travail de modernisation ayant abouti à l'adoption par le Comité des ministres du Conseil de l'Europe, le 18 mai 2018, à Elseneur, Danemark, du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), disponible à l'adresse https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168076c65c0. Sur ce nouveau texte, voy. C. DE TERWANGNE, « Privacy and Data Protection in Europe : Council of Europe and European Union Legislations », in *Research Handbook on Privacy and Data Protection Law*, Londres, Edward Elgar, 2019 (à paraître).

4 Cap-Vert, Maurice, Mexique, Sénégal, Tunisie, Uruguay.

5 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), *J.O.U.E.*, L 119/1, 4 mai 2016. Sur ce texte, voy. C. DE TERWANGNE et K. ROSIER (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, coll. du CRIDS, Bruxelles, Larcier, 2018 ; Y. POULLET, « Le nouveau règlement général européen de la protection des données (en abrégé RGPD) est arrivé », *Tax, Audit and Accountancy*, décembre 2017, n° 57, pp. 6-24, disponible à l'adresse https://www.ibr-ire.be/nl/DocumetsMailings/TAA-57.pdf ; V. VERBRUGGEN, « Mise en œuvre du Règlement général sur la protection des données : coup de projecteur sur certaines nouvelles obligations à charge des responsables de traitement et des sous-traitants », *Ors.*, 2017, liv. 5, pp. 2-22 ; C. PONSART et R. ROBERT, « Le règlement européen de protection des données personnelles », *J.T.*, 2018, pp. 421-438 ; K. JANSSENS et M. NUYTTEN, « De Algemene Verordening Persoonsgegevens : van theorie naar praktijk. Le Règlement Général sur la Protection des Données : de la théorie à la pratique », *R.D.C.*, 2018, pp. 401-435 ; E. DEGRAVE, « Le règlement général sur la protection des données et le secteur public », *Rev. dr. commun.*, 2018, pp. 4-14 ; A. BANKS, « GDPR/RGPD : pourquoi tant d'effervescence autour de ces quatre lettres ? », *Entertainment*, 2018/3, pp. 159-178. ; S. PEYROU, « Le nouveau règlement général européen relatif à la protection des données à caractère personnel : un texte à la hauteur de ses ambitions », *R.A.E.*, 2016, pp. 103-110 ; B. DOCQUIR (éd.), *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017 ; A. BENSOUSSAN, J. HENROTTE, M. GALLARDO et S. FANTI, *General Data Protection Regulation. Texts, Commentaries and Practical Guidelines*, Malines, Wolters Kluwer Belgium, 2017 ; N. RAGHENO (éd.), *Data*



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



application depuis le 25 mai 2018, a lui aussi une portée dépassant les frontières européennes. Son champ d'application territorial englobe en effet les acteurs économiques situés hors de l'Union européenne mais offrant des biens ou des services destinés à un public cible localisé dans l'UE[6].

Les pages qui suivent offrent une analyse des règles et principes contenus dans ces nouveaux instruments juridiques, analyse nourrie également des éclairages tirés de la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne (points III, IV et V, *infra*). Sur le continent européen, la protection des données personnelles est érigée en véritable droit fondamental, au service d'autres droits et libertés (point II), ou en conflit avec ces droits (point VI). La société née des développements technologiques s'identifie insidieusement à un « société de surveillance », sur laquelle on se penchera pour clore le propos (partie VII).

### C. – *La notion de donnée à caractère personnel*

Avant d'entamer l'analyse, il s'impose de clarifier ce que recouvre la notion de « donnée à caractère personnel » (aussi appelée « donnée » ci-après, par souci de lisibilité). Tant le RGPD que la Convention 108+ spécifient que cette notion englobe toute information se rapportant à une personne physique identifiée ou identifiable[7]. Il s'agit donc d'un concept particulièrement large puisque, loin de se limiter aux informations privées ou confidentielles, il s'applique à l'égard de n'importe quelle information – également publique ou professionnelle – pourvu que cette information puisse être rattachée directement ou indirectement[8] à un individu vivant[9]. La donnée à caractère personnel couvre toute forme d'information (écrits, photos, sons, données de localisation, données de comportement en ligne, adresses IP[10], données biométriques, etc.). Elle couvre également tant les données qui résultent d'éléments objectifs, vérifiables et contestables, que

*Protection & Privacy. Le GDPR dans la pratique. [General Data Protection Regulation – Règlement général sur la protection des données]*, Limal, Anthemis, 2017 ; A. BEELEN, *Guide pratique RGPD. Fiches de guidance*, Bruxelles, Bruylant, 2018.

6 C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *Journal de droit européen*, 2017, pp. 302 et s.

7 Art. 4.1 du RGPD ; art. 2.a de la Convention 108 modernisée (ci-après Convention 108+).

8 Le rattachement peut se faire par le biais d'un numéro d'identification, d'un identifiant en ligne, de données de localisation ou par un ou plusieurs éléments physiques, génétiques, psychiques, économiques, culturels ou sociaux.

9 Voy. considérant 27 du RGPD.

10 C.J.U.E., 24 novembre 2011, *Scarlett c. SABAM*, C-70/10, pt 51 ; C.J.U.E., 19 octobre 2016, *Breyer c. Allemagne*, C-582/14, pt 49 : « une adresse IP dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site internet que ce fournisseur rend



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



les données subjectives contenant une évaluation ou un jugement porté sur quelqu'un[11]. Ce qui importe c'est que la personne à laquelle se rapporte l'information soit identifiée ou identifiable. L'identification dont il est question doit se comprendre non comme l'établissement de l'identité civile d'un individu mais comme *l'individualisation* de cette personne, la capacité de la traiter différemment des autres[12].

## II. Le droit à la protection des données, un droit fondamental

La protection des données est considérée en Europe comme un droit fondamental autonome mais étroitement lié au droit à la protection de la vie privée (A). On verra ci-dessous que la protection des données est également liée à d'autres droits fondamentaux, en tant que condition d'exercice de ces droits (B). Elle est aussi intrinsèquement liée à la dignité des individus (C).

### A. – *Lien entre droit à la vie privée et droit à la protection des données*

Dans le contexte des technologies de l'information et de la communication, et spécifiquement d'Internet, la notion de vie privée a été amenée à évoluer et ne doit pas se comprendre de façon traditionnelle comme limitée à une sphère intime à protéger, contenant un ensemble d'informations privées, voire confidentielles, que l'on souhaite garder cachées. Elle est à entendre comme faculté d'autodétermination, d'autonomie, capacité de l'individu à effectuer des choix existentiels[13]. En la matière, il s'agit plus précisément d'autodétermination informationnelle[14], c'est-à-dire de la

accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à internet de cette personne ».

11 C.J.U.E., 20 décembre 2017, *Novak*, C-434/16, pt 34.

12 Voy. le considérant 36 du RGPD et le § 18 du rapport explicatif de la Convention 108+.

13 Pour la reconnaissance explicite d'un droit à l'autodétermination ou l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'art. 8 CEDH, voy. Cour eur. D.H., 7 mars 2006, *Evans c. Royaume-Uni* (confirmé par la Grande chambre dans son arrêt du 10 avril 2007) ; 20 mars 2007, *Tysiac c. Pologne* ; 1er juillet 2008, *Daroczy c. Hongrie*.

14 Voy. H. BURKERT, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *Droit de l'Informatique et des Télécoms*, 1985, pp. 8-16 ; E. DEGRAVE et A. LACHAPELLE, « Le droit d'accès du contribuable à ses données à caractère personnel et la lutte contre la fraude fiscale », note sous C.C., 27 mars 2014, *R.G.C.F.*, 2014, p. 325 ; C. DE TERWANGNE, « La difficile application de la législation de protection des données à caractère personnel », *J.T.*, 2017, p. 752 ; A. ROUVROY et Y. POULLET, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie », in *État de droit et virtualité* (K. BENYEKHLEF et P. TRUDEL eds.), Montréal, Thémis, 2009, pp. 157-222, http://www.crid.be/pdf/public/6050.pdf.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



possibilité pour l'individu de « savoir ce qui se sait sur lui », de connaître les données le concernant qui sont détenues par autrui, d'en maîtriser les circuits de communication, d'en contrecarrer les utilisations abusives[15]. La vie privée ne se réduit donc pas à une quête de confidentialité, c'est la maîtrise par chacun de son image informationnelle.

La Cour européenne des droits de l'homme a expressément reconnu dans son récent arrêt *Satamedia*[16] qu'un droit à l'autodétermination informationnelle était attaché au droit à la protection de la vie privée. Elle a ainsi établi que « [l]a protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention [européenne des droits de l'homme]. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article […]. L'article 8 de la Convention consacre donc le *droit à une forme d'auto-détermination informationnelle*, qui autorise les personnes à invoquer leur droit à la vie privée en ce qui concerne des données qui, bien que neutres, sont collectées, traitées et diffusées à la collectivité, selon des formes ou modalités telles que leurs droits au titre de l'article 8 peuvent être mis en jeu »[17].

La Convention 108 modernisée du Conseil de l'Europe, destinée à remplacer la version de 1981, s'inscrit dans la même ligne puisqu'elle affirme solennellement dans son préambule : « qu'il est nécessaire de garantir la dignité humaine ainsi que la protection des droits de l'homme et des libertés fondamentales de toute personne, et, eu égard à la diversification, à l'intensification et à la mondialisation des traitements des données et des flux de données à caractère personnel, *l'autonomie personnelle, fondée sur le droit de toute personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait* »[18–19].

En résumé, la protection des données est une émanation du droit au respect de la vie privée pris dans la dimension de droit à

15 Voy. F. RIGAUX, *La vie privée : une liberté parmi les autres ?*, coll. Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 588 et 589, n° 532. Voy. également Cour eur. D.H., 26 mars 1987, *Leander c. Suède*, *Publ. Cour*, série A, n° 116 ; Cour eur. D.H. (Gde ch.), 4 décembre 2008, *S. et Marper c. Royaume Uni*.

16 Cour eur. D.H. (Gde ch.), 27 juin 2017, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*.

17 *Ibid.*, § 137.

18 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), précité.

19 Voy. déjà en 1998 : Rés. 1165 (1998) de l'Assemblée parlementaire du Conseil de l'Europe sur le droit au respect de la vie privée, adoptée le 26 juin 1998 : « [p]our tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition [du droit au respect de la vie privée] *le droit de contrôler ses propres données* » (nos italiques).



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



l'autodétermination qui y est liée. C'est le droit pour chacun de contrôler ses propres données, qu'elles soient intimes et privées mais aussi professionnelles ou publiques, soit « neutres » pour reprendre les termes de la Cour européenne des droits de l'homme.

Le droit à la protection des données à caractère personnel a été reconnu comme droit fondamental à part entière à l'article 16 du TFUE ainsi que dans la Charte des droits fondamentaux de l'Union européenne. Cette dernière distingue en effet explicitement le droit au respect de la vie privée (article 7) du droit à la protection des données à caractère personnel (article 8)[20].

L'élévation de la Charte au rang des sources du droit primaire de l'Union à partir du 1er décembre 2009 a entrainé la reconnaissance de la protection des données à caractère personnel comme droit fondamental autonome par la Cour de justice de l'Union européenne[21]. Cela étant, la Cour estime que ce droit est étroitement lié au droit au respect de la vie privée[22]. Ainsi, dans l'affaire *Digital Rights Ireland*[23], elle a prononcé l'invalidité de la directive relative à la conservation des données de trafic (directive 2006/24[24]) pour violation des articles 7 et 8 de la Charte des droits fondamentaux consacrant ces deux droits. Elle a en effet relevé que la conservation des données de trafic (données liées à l'usage du téléphone fixe, mobile, de la téléphonie sur Internet et à l'usage d'Internet dans son ensemble) permettait de tirer des conclusions très précises concernant la vie privée des personnes dont les données sont conservées, telles que « les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »[25]. En conséquence, elle a estimé que « [l]a conservation des données aux fins de leur accès

20 La Charte des droits fondamentaux de l'UE, art. 7 : « [t]oute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications » ; art. 8 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant ; 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ; 3. Le respect de ces règles est soumis au contrôle d'une autorité de protection des données ».

21 C.J.U.E. (Gde. ch.), 9 novembre 2011, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, aff. jointes C-92/09 et C-93/09.

22 *Ibid*., pt 47 et C.J.U.E., 24 novembre 2011, *ASNEF et FECEMD c. Administracion del Estato*, aff. jointes C-468/10 et C-469/10, pt 41.

23 C.J.U.E. (Gde. ch.), 8 avril 2014, *Digital Rights Ireland*, aff. jointes C-293/12 et C-594/12.

24 Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, *J.O.U.E.*, L 105, p. 54.

25 C.J.U.E. (Gr. ch.), *Digital Right Ireland*, préc., pt 27.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



éventuel par les autorités nationales compétentes, telle que prévue par la directive 2006/24, concerne de manière directe et spécifique la vie privée et, ainsi, les droits garantis par l'article 7 de la Charte. En outre, une telle conservation des données relève également de l'article 8 de celle-ci en raison du fait qu'elle constitue un traitement des données à caractère personnel au sens de cet article et doit, ainsi, nécessairement satisfaire aux exigences de protection des données découlant de cet article »[26]. Dans l'affaire *Schrems*, la Cour va jusqu'à évoquer ces deux droits de manière particulièrement entremêlée : elle relève le « rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée »[27] et établit que « la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire »[28].

### B. – *Lien entre droit à la protection des données et autres droits et libertés*

Le droit à la protection des données est intrinsèquement lié à l'exercice d'autres droits et libertés. Dans une série de situations, protéger les données à caractère personnel revient à favoriser la jouissance et l'exercice de ces droits et libertés[29].

Ainsi, les traitements de données peuvent avoir un impact sur la liberté d'association. Comme l'a exprimé la Cour constitutionnelle allemande dans son fameux arrêt de 1983 concernant le recensement de population, « [u]ne personne qui suppose […] que sa participation à une réunion ou à une initiative citoyenne est officiellement enregistrée et qu'elle est donc susceptible de lui occasionner des problèmes, peut décider de renoncer à l'exercice de ses droits fondamentaux »[30]. Le sort

26 *Ibid.*, pt 29. Voy. égal. C.J.U.E., 9 novembre 2011, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, pt 47 ; C.J.U.E., 13 Mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12, pt 38.

27 C.J.U.E., 6 octobre 2015, *Schrems c. DPC Irlande*, C-362/14, pt 78. La Cour européenne des droits de l'homme s'est exprimée dans les mêmes termes à plusieurs reprises, not. Cour eur. D.H. (Gde ch.), 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103 : « [l]a protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée ».

28 *Ibid.*, pt 92.

29 Inversement, la protection des données peut aussi entrer en conflit avec d'autres droits et libertés : notamment avec la liberté d'expression (voy. C.J.U.E., *Lindqvist* et *Satamedia* ; voy. *infra*, VI, B), le droit à l'information (C.J.U.E., *Google Spain* ; voy. *infra*, pt III, C, 2), avec le droit de propriété et le droit à un recours effectif (C.J.U.E., *Promusicae* ; voy. *infra*, VI, A), ou avec le droit économique de l'employeur (Cour eur. D.H., 5 septembre 2017, *Barbulescu c. Roumanie* ; voy. *infra*, pt VII, C).

30 Cour constitutionnelle allemande (*BundesVerfassungsGericht*), 15 décembre 1983, *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 ff.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



des fichiers des membres de groupes et d'associations peut clairement influer sur l'adhésion à ces groupes et la participation à leurs initiatives. L'effet se fait ressentir non seulement à un niveau individuel, en termes de liberté d'action des individus, mais également à un niveau collectif, impactant le bien commun. Selon la Cour constitutionnelle allemande, en effet, « Cela limiterait non seulement les possibilités d'épanouissement personnel de l'individu, mais aussi le bien commun dans la mesure où l'autodétermination est une condition essentielle à l'existence d'une société libre et démocratique qui repose sur les capacités et la solidarité de ses citoyens »[31].

La protection des données est également en lien évident avec la liberté de s'informer et de s'exprimer. Ainsi, si un individu se sait potentiellement surveillé au vu des traces gardées systématiquement par la technologie de ses messages et actions sur le Web, comment pourrait-il exercer sans état d'âme sa liberté d'expression et d'information[32] ? Par ailleurs, l'exercice de cette liberté impose de ne pas voir les informations filtrées en fonction de profils préétablis. Il est crucial que tout le monde puisse accéder à l'ensemble de l'information disponible. Or, l'épisode du Brexit a mis au jour les pratiques des réseaux sociaux (à tout le moins de Facebook) dont les algorithmes sélectionnent précisément l'information pour chacun des membres, réservant, dans le cas du Brexit, aux uns une information en faveur du « *leave* » et aux autres une information soutenant le « *remain* ». Cette façon de procéder a clairement influencé la campagne du Brexit et son résultat, et c'est véritablement le fonctionnement démocratique qui en a été remis en cause. Le cas de la campagne britannique n'est hélas pas isolé et dans d'autres situations, l'exploitation camouflée de données personnelles a gravement impacté l'exercice du droit de vote.

D'autre part, la liberté de se déplacer implique la maitrise de ses données de géolocalisation. L'individu porteur d'un téléphone ou d'une montre connectés enregistrant tous ses déplacements et envoyant ces données dans le *cloud* aux offreurs de services mais également à leurs partenaires, a un intérêt certain à voir ses données protégées et à se voir octroyer des droits à l'égard des différents intervenants. Les mêmes préoccupations sont liées aux déplacements par des moyens de transports

31 *Ibid.*

32 Y. POULLET, J.-M. DINANT, C. DE TERWANGNE et M.-V. PEREZ-ASINARI, *L'autodétermination informationnelle à l'ère de l'Internet*, rapport pour le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Strasbourg, Conseil de l'Europe, 18 novembre 2004.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



en commun laissant des traces entre les mains d'acteurs tiers, par le biais des cartes à puce désormais généralisées en remplacement des traditionnels tickets en carton, bien moins bavards que leurs remplaçantes connectées. Et les caméras disséminées le long des routes et dans les villes veillent, elles aussi, à témoigner du passage des usagers. Le sort de toutes ces données a une incidence indubitable sur l'exercice de la liberté de mouvement.

Enfin, et sans prétendre clore cette liste, le droit à la non-discrimination est directement mis en cause par les opérations de profilage des individus. C'est alors, par exemple, le droit de se loger ou de trouver un emploi dans les mêmes conditions que les autres qui entre en jeu. Mais également le droit de ne pas voir les prix varier en fonction du profil de consommateur. Ou encore, le droit de ne pas être étiqueté, par l'intervention d'un algorithme, candidat fraudeur ou délinquant, sans fondement légitime.

### C. – *Lien entre droit à la protection des données et dignité*

Ainsi qu'on le voit dans l'extrait du Préambule de la Convention 108 modernisée cité plus haut, les auteurs du texte ont été soucieux de mettre en exergue la nécessité de garantir la dignité humaine face à la multiplication et l'intensification des traitements de données à caractère personnel. Il s'agit de rappeler que l'être humain doit demeurer un sujet et non être réduit à un simple objet de surveillance, de contrôle ou de déductions algorithmiques. Le rapport explicatif de la Convention 108 modernisée l'affirme en ces termes : « [l]a dignité humaine requiert la mise en place de garanties lors du traitement de données à caractère personnel, afin que les individus ne soient pas traités comme de simples objets »[33].

L'atteinte à la dignité est par ailleurs clairement et à plusieurs reprises invoquée dans la recommandation du Comité des ministres du Conseil de l'Europe concernant la protection des données dans le contexte du profilage[34], contexte particulièrement, mais pas exclusivement, lié à Internet. Deux considérants de ce texte sont très explicites : « [c]onsidérant que l'utilisation de profils, même de manière légitime, sans précautions ni

33 § 10, *in fine*, du rapport explicatif de la Convention 108+.

34 Recommandation CM/Rec(2010) 13 du 23 novembre 2010 du Comité des ministres du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



garanties particulières, est susceptible de porter gravement atteinte à la dignité de la personne de même qu'à d'autres libertés et droits fondamentaux, y compris aux droits économiques et sociaux » et « [c]onsidérant que la protection de la dignité humaine et d'autres droits et libertés fondamentaux dans le cadre du profilage ne peut être effective que si, et seulement si, toutes les parties prenantes contribuent ensemble à un profilage loyal et licite des individus ».

Au niveau de l'Union européenne, le RGPD ne mentionne pas explicitement la dignité humaine mais, dans les tout premiers considérants de ce texte, les législateurs de l'Union européenne évoquent indirectement cette valeur et l'idée que la machine doit rester au service de l'homme : « [l]e traitement des données à caractère personnel devrait être conçu pour servir l'humanité »[35].

Cette proclamation de la valeur fondamentale de la dignité humaine dans les textes du Conseil de l'Europe et l'injonction de concevoir les traitements de données au service de l'humanité sont sans aucun doute particulièrement nécessaires aujourd'hui. C'est notamment dans l'exigence que le sort d'un individu ne soit pas exclusivement décidé par un logiciel[36] que se traduira la protection de la dignité humaine.

## III. Le régime de protection des données à caractère personnel

Sur Internet comme ailleurs, les données à caractère personnel sont protégées. Le fait que les données soient diffusées, donc publiques, ne les fait pas sortir du champ de la protection, qu'elles le soient spontanément par les personnes concernées elles-mêmes ou qu'elles fassent l'objet d'une publication par un tiers sur un site Web[37]. Par ailleurs, de multiples données à caractère personnel sont aussi récoltées dans le sillage de la navigation des internautes, sans connaitre de publicité et la

35 Considérant 4 du RGPD.

36 Voy. *infra* dans la section IV consacrée aux droits des personnes concernées, l'évocation du droit de ne pas être soumis à une décision entièrement automatisée.

37 Pour cette dernière hypothèse, voy. l'affirmation claire, à l'occasion de la même affaire, de la Cour de justice tout d'abord (C.J.C.E., 16 décembre 2008, C-73/07, *Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia oy*, pt 48 : « il y a lieu de relever qu'une dérogation générale à l'application de la directive [95/46] en faveur d'informations publiées viderait cette dernière largement de son sens. En effet, il suffirait aux États membres de faire publier des données pour les faire échapper à la protection prévue par la directive ») puis de la Cour européenne des droits de l'homme (Cour eur. D.H. (Gde ch.), *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, préc., § 34 : « [l]e fait que les informations en cause sont déjà dans le domaine public ne les soustrait pas nécessairement à la protection de l'article 8 »).



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



plupart du temps à l'insu des personnes concernées. Elles n'en méritent pas moins de bénéficier du régime de protection.

La protection des données se décline en un catalogue de principes et d'exigences centrés sur le respect de la proportionnalité, de la finalité, de la transparence et de la sécurité. Une série de droits garantissent aux personnes concernées leur information et dès lors leur pouvoir de décision, d'action et de surveillance quant au sort réservé à leurs données.

## A. – *Respect du principe de proportionnalité et nécessité d'un fondement légitime*

### 1. – *Respect du principe de proportionnalité*

Dès son tout premier arrêt en matière de protection des données, la Cour de justice de l'Union européenne a mis en exergue le fait que la mise en œuvre d'un traitement de données doit respecter l'exigence de proportionnalité[38]. L'ingérence induite par un traitement de données doit en conséquence être nécessaire, dans une société démocratique, pour atteindre le but légitime poursuivi, ce qui implique que la mesure prise soit « proportionnée au but légitime recherché »[39]. Il convient donc de « mettre en balance l'intérêt [poursuivi par le traitement des données] avec la gravité de l'atteinte au droit des personnes concernées au respect de leur vie privée [provoquée par le traitement des données] »[40].

La Cour de justice a eu de multiples occasions de réitérer cette exigence du respect du principe de proportionnalité pour qu'un traitement de données à caractère personnel soit admissible[41]. Une des plus célèbres de ces occasions concerne l'affaire *Digital Rights Ireland*[42] qui débouchera sur l'invalidation spectaculaire de la directive 2006/24 imposant la rétention des données relatives aux communications électroniques, huit ans après l'adoption de celle-ci, pour non-respect de l'exigence de proportionnalité. La Cour confirmera sa condamnation de la conservation généralisée et indifférenciée des données de

38 C.J.C.E., 20 mai 2003, *Österreichischer Rundfunk*, aff. jointes C-465/00, C-138/01 et C-139/01, pt 83.
39 *Ibid.*, pt 83.
40 *Ibid.*, pt 84.
41 Voy. not. à propos de l'obligation de publication des coordonnées de tous les bénéficiaires des fonds agricoles européens, considérée comme ne respectant pas le principe de proportionnalité : C.J.U.E., 9 novembre 2010, *Volker and Markus Schecke GbR and Hartmut Eifert c. Land Hessen*, aff. jointes C-92/09 et C-93/09, pts 86 et 89.
42 C.J.U.E., 8 avril 2014, *Digital Rights Ireland*, aff. jointes C-293/12 et C-594/12.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



communication, dans son arrêt *Tele2 Sverige* du 21 décembre 2016[43] (voy. *infra*, point VII, B).

La Cour européenne des droits de l'homme exige, elle aussi, qu'un juste équilibre soit respecté entre les intérêts publics et privés en concurrence lorsqu'un traitement de données est mis en place. Dans son arrêt *S. et Marper*, la Cour a ainsi affirmé que la conservation des données en cause (des empreintes digitales, échantillons cellulaires et profils ADN) doit être proportionnée et refléter le juste équilibre en question[44].

Dans sa version de 1981, la Convention 108 n'exige pas explicitement que le traitement des données respecte la proportionnalité. Elle n'évoque l'exigence de proportionnalité que concernant les données à caractère personnel qui font l'objet du traitement, dans la mesure où celles-ci ne peuvent être « excessives par rapport aux finalités pour lesquelles elles sont enregistrées »[45]. Lors de la révision de la Convention, il est apparu impératif d'exiger le respect du principe de proportionnalité non plus pour les seules données mais pour le traitement en tant que tel et tout ce qu'il est envisagé de faire avec les données. Cela permet d'offrir un rempart contre les risques découlant des pratiques liées aux développements techniques (notamment la multiplication des traitements de données insoupçonnés sur Internet).

La Convention 108+ stipule désormais expressément cette exigence de proportionnalité pour l'ensemble du traitement de données. Aux termes de son article 5, paragraphe 1er, « [l]e traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu ». Le rapport explicatif apporte cet éclairage que pour être proportionné, le traitement doit être pertinent au regard de la finalité légitime poursuivie, et limité à ce qui est nécessaire au regard des intérêts, droits et libertés des personnes concernées ou de l'intérêt public. Il ne doit pas induire une ingérence disproportionnée dans ces intérêts, droits et libertés[46].

43 C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department c. Tom Watson e.a.*, aff. jointes C-698/15 et C-203/15.

44 Cour eur. D.H., 4 décembre 2008, *S. and Marper c. UK*, § 118. Voy. également Cour eur. D.H. (Gde ch.), 4 mai 2000, *Rotaru c. Roumanie*.

45 Art. 5, c), de la Convention 108.

46 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), rapport explicatif, 18 mai 2018, § 40.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



Il est à noter que le principe de proportionnalité doit être respecté à toutes les étapes du traitement, « y compris au stade initial, c'est-à-dire lorsqu'il est décidé de procéder ou non au traitement des données »[47].

### 2. – *Nécessité d'un fondement légitime*

Pour être admis, tout traitement de données doit donc respecter le principe de proportionnalité mais il doit également[48] reposer sur un fondement légitime admis par les textes de protection des données[49]. Certains de ces fondements méritent qu'on s'y attarde dans le cadre d'une réflexion sur les traitements de données dans le contexte d'Internet.

Le premier fondement est le consentement de la personne concernée. Sur Internet, les individus peuvent par exemple consentir à ce que leurs photos soient diffusées sur des réseaux sociaux ou sur la page Web d'une école, ou à ce que des commentaires signés de leur nom soient publiés sur des forums ou encore à ce que des cookies soient enregistrés sur leur ordinateur ou téléphone, en vue de récolter des informations relatives à leurs sessions de navigation.

Pour être valable, le consentement doit être libre (c'est-à-dire émis sans pression), spécifique[50] (il ne peut être général et doit porter sur un traitement de données précis), éclairé (la personne a reçu toute l'information utile sur le traitement envisagé ; elle doit notamment savoir qui utilisera ses données et pourquoi, et se rendre compte des destinataires de ses données) et non équivoque[51]. « Un tel consentement doit représenter la libre expression d'un choix intentionnel »[52]. Il doit manifester la volonté de la personne concernée par une déclaration ou un acte positif clair de sa part. « Le silence, l'inaction ou des formulaires ou cases à cocher prévalidés ne peuvent constituer un consentement »[53].

47 *Ibid*.

48 Voy. le rapport explicatif de la Convention 108+, préc., § 41 *in fine* : « [l]es paragraphes 1 [respect du principe de proportionnalité], 2 [exigence d'un fondement légitime], 3 et 4 de l'article 5 sont cumulatifs et doivent être respectés pour garantir la légitimité du traitement des données ».

49 Art. 6 du RGPD ; art. 5, § 2 de la Convention 108 modernisée.

50 Voy. C.J.U.E., 5 mai 2011, *Deutsche Telekom AG c. Allemagne*, C-543/09, pts 61-62.

51 Art. 4, 11°, du RGPD ; rapport explicatif de la Convention 108+, § 42.

52 Rapport explicatif de la Convention 108+, § 42.

53 *Ibid*. Le fait que les éditeurs de sites Web ont la faculté d'indiquer aux moteurs de recherche, à l'aide de protocoles d'exclusion comme « robot.txt » ou de codes comme « noindex » ou « noarchive », qu'ils souhaitent qu'une information particulière, publiée sur leur site, soit exclue des index automatiques de ces moteurs ne signifie pas que l'absence d'une telle indication de la part de ces éditeurs correspond à un consentement à ce que les données soient traitées (C.J.U.E., 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12, pt 39).



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



Le rapport explicatif de la Convention 108+ spécifie que « [l]'expression d'un consentement ne dispense pas de respecter les principes fondamentaux de la protection des données à caractère personnel énoncés au chapitre II de la Convention : la proportionnalité du traitement, par exemple, doit toujours être considérée »[54]. Par cette précision, les auteurs de la Convention 108+ soulignent que la vérification du respect de la proportionnalité lors du traitement de données devra toujours être faite, même en présence du consentement des personnes concernées à ce qu'on traite leurs données. Si la présence d'un consentement permet de présumer la légitimité d'un traitement, la mise en balance des intérêts en présence et la vérification de l'équilibre atteint offre une sauvegarde bienvenue quand on songe aux défauts trop souvent attachés au consentement (information insuffisante de la personne concernée, manifestation du consentement déduite de la non-modification de conditions par défaut, nécessité de consentir à l'ensemble des traitements des données annoncés si l'on veut accéder au service souhaité, etc.).

La deuxième base de légitimité réside dans la nécessité du traitement des données pour l'exécution d'un contrat ou de mesures précontractuelles[55]. C'est le cas très fréquent de la collecte de données pour permettre l'utilisation d'un service en ligne ou d'une application, pour passer commande, faire des achats ou des enchères sur Internet, etc. Il est important dans tous ces cas, de limiter le traitement aux seules données réellement nécessaires pour exécuter le contrat en question.

Le traitement des données est aussi admis quand il est exigé par une loi ou lorsqu'il s'inscrit dans le cadre d'une mission publique[56]. Ainsi, par exemple, depuis le déploiement de l'e-gouvernement et de l'offre de services publics en ligne, Internet est devenu l'instrument privilégié du dialogue entre l'administration et le citoyen, dialogue bien souvent nourri de données à caractère personnel. Le considérant 41 du RGPD précise que la base juridique ou la mesure législative qui sert de fondement au traitement de données doit répondre aux exigences mises en lumière par la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne. Elle doit en conséquence être claire et précise et son application doit être prévisible pour les justiciables. Les finalités des traitements en cause doivent être définies dans cette base juridique ou être liées à la mission d'intérêt

54 *Ibid.*, pt 44.
55 Art. 6, § 1er, b), du RGPD ; § 46 du rapport explicatif de la Convention 108+.
56 Art. 6, § 1er, d) et e), du RGPD ; §§ 46 et 47 du rapport explicatif de la Convention 108+.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



public en question[57]. Ici aussi, seul le traitement des données véritablement nécessaires pour atteindre la finalité poursuivie est admis. Ainsi, la Cour de justice a eu l'occasion de préciser dans l'affaire *Huber* qu'un registre centralisé contenant des données à caractère personnel relatives aux citoyens de l'Union non-ressortissants allemands et consultable par différentes entités publiques et privées aux fins de l'application de la réglementation sur le droit de séjour, ne répond à l'exigence de nécessité que s'il ne contient que les données nécessaires à l'application par ces autorités de cette réglementation et si son caractère centralisé permet une application plus efficace de cette réglementation en ce qui concerne le droit de séjour des citoyens de l'Union non-ressortissants de cet État membre[58]. La Cour a en outre affirmé que, s'agissant des modalités d'utilisation d'un tel registre, seul l'octroi d'un accès à des autorités ayant compétence dans le domaine de la réglementation sur le droit de séjour pouvait être considéré comme nécessaire[59] et qu'elle n'admettait par contre pas comme nécessaire la conservation des données en question à des fins statistiques[60].

Enfin, la dernière hypothèse de traitement légitime à mentionner concerne le traitement des données nécessaires à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée[61]. Cette dernière hypothèse correspond à une mise en balance des intérêts et droits en présence. Il revient dans un premier temps au responsable du traitement d'effectuer lui-même la mise en balance et, s'il estime que la mise en œuvre du traitement de données qu'il envisage sert un intérêt supérieur à celui de la personne concernée ainsi qu'aux droits et libertés de celle-ci, il conclura que son traitement est légitime. La personne concernée pourra, quant à elle, contester le résultat de cette mise en balance et estimer que ses intérêts, droits et libertés prévalent sur l'intérêt poursuivi par le responsable. Elle se voit octroyer pour ce faire un droit d'opposition[62].

La Cour de justice de l'UE a admis que lors de la pondération des intérêts en présence, « la gravité de l'atteinte aux droits fondamentaux

57 Art. 6, § 3, al. 2, du RGPD.
58 C.J.C.E. (Gde ch.), 16 décembre 2008, *Huber c. Allemagne*, C-524/06, pt 66.
59 *Ibid*., pt 61.
60 *Ibid*., pt 68.
61 Art. 6, § 1er, f), du RGPD ; § 46 du rapport explicatif de la Convention 108+.
62 Art. 21 du RGPD ; art. 9, § 1er, d), de la Convention 108+.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



de la personne concernée par ledit traitement peut varier en fonction du fait de savoir si les données en cause figurent déjà, ou non, dans des sources accessibles au public »[63]. Mais la Cour estime que l'on ne peut exclure de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées[64].

Le traitement effectué par les moteurs de recherches lorsqu'ils font apparaitre dans la liste des résultats des informations ou des photos sur des personnes physiques correspond à cette hypothèse de légitimité. De même que les publications de données à caractère personnel par les sites de presse, que ce soit sous forme d'écrits, de photos ou de vidéos. Ces traitements sont légitimes lorsque l'intérêt de la liberté de presse et du droit à l'information du public l'emporte sur les droits à la vie privée, à l'image ou à l'honneur des personnes mentionnées sur les sites en question.

### 3. – *Données sensibles*

Certaines informations personnelles sont par nature beaucoup plus sensibles que d'autres. Alors que le nom et l'adresse de quelqu'un sont des informations somme toute anodines, il n'en est pas de même des convictions politiques de cette personne, de sa santé ou de son passé judiciaire. Un régime plus protecteur que pour les données ordinaires est réservé à ces données, étant donné le risque plus élevé que leur traitement engendre pour la personne concernée[65]. Tant la Convention 108 modernisée que le RGPD ont repris, en l'étoffant quelque peu la liste des données sensibles figurant dans la Convention 108 de 1981 et dans la directive 95/46. Ainsi, à côté des données qui révèlent l'origine raciale et ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale et les données concernant la santé et la vie sexuelle, figurent désormais aussi l'orientation sexuelle, les données génétiques et les données biométriques traitées aux fins d'identifier une personne physique de manière unique[66]. À cette liste on peut ajouter les données relatives aux condamnations pénales et aux infractions ou mesures de sûreté connexes[67].

63 C.J.U.E., 24 novembre 2011, *ASNEF et FECEMD c. Administracion del Estado*, aff. jointes C-468/10 et C-469/10, pt 44.
64 *Ibid*., pts 48 et 49.
65 Art. 6 de la Convention 108+ ; art. 9 du RGPD.
66 Art. 6 de la Convention 108+ ; art. 9 du RGPD.
67 Art. 6, § 1er, de la Convention 108+ ; art. 10 du RGPD.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



La Cour européenne des droits de l'homme a insisté sur le caractère sensible voire très sensible, de plusieurs types de données, telles les données médicales[68], notamment les données relatives à la séropositivité[69] ou à un avortement[70], les données génétiques et biométriques. Elle a estimé que « la conservation d'empreintes digitales constitue une atteinte au droit au respect de la vie privée »[71] qui ne peut donc être admise que moyennant le respect des conditions du paragraphe 2 de l'article 8 de la Convention européenne des droits de l'homme. Selon la Cour, « le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs. Les considérations qui précèdent valent tout spécialement lorsqu'est en jeu la protection de catégories particulières de données plus sensibles, notamment des données ADN, qui, dans la mesure où elles contiennent le patrimoine génétique de la personne, revêtent une grande importance tant pour elle-même que pour sa famille »[72].

### B. – *Exigence de loyauté et transparence*

L'exigence de loyauté[73] induit que le traitement des données soit réalisé dans la transparence pour les personnes concernées, et sans tromperie. Les traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données[74], d'une manière qui serait tout à fait inattendue ou imprévisible pour elles. Les personnes concernées doivent, en pleine connaissance de cause, pouvoir établir une relation de confiance avec ceux qui traitent leurs données à caractère personnel[75]. Cette loyauté du traitement des données ne se limite pas à la collecte, mais doit être garantie à toutes les étapes du traitement[76].

68 Cour eur. D.H., 25 février 1997, *Z. c. Finlande* ; 6 juin 2013, *Avilkina c. Russie* ; 15 avril 2014, *Radu c. Moldavie*, § 27.

69 Cour eur. D.H., 25 novembre 2008, *Armonienė c. Lituanie* et *Biriuk c. Lituanie*.

70 Cour eur. D.H., 27 août 1997, *M.S. c. Suède* ; 23 février 2016, *Y.Y. c. Russie*.

71 Cour eur. D.H. (Gde ch.), 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103.

72 *Ibid*., § 103.

73 « Les données à caractère personnel doivent être traitées de manière loyale et transparente au regard de la personne concernée » (art. 5, § 1er, a), du RGPD) ; également art. 5, § 4, a), de la Convention 108+.

74 Cour eur. D.H., 3 avril 2007, *Copland c. Royaume Uni*.

75 E. DEGRAVE, « Le Règlement général sur la protection des données et le secteur public », *Rev. dr. commun.*, 2018, pp. 4 et 5. Également Groupe de l'Article 29, Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018, WP 260rev01, § 2 : « [*t*]*ransparency* […] *is about engendering trust in the processes which affect the citizen by enabling them to understand, and in necessary, challenge those processes* ».

76 Groupe de l'Article 29, Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018, WP 260rev01, § 5.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



C'est un problème de loyauté qui fut au cœur du scandale « Cambridge Analytica »[77] : les utilisateurs de Facebook étaient invités à répondre à un test de personnalité pour lequel ils étaient amenés à croire qu'ils opéraient dans le cadre d'une étude universitaire et que le but poursuivi était dès lors académique, alors qu'en réalité l'objectif de la récolte des données était commercial et de prospection politique.

Le principe de loyauté est donc lié au droit à la transparence[78]. Ce droit à la transparence implique que certaines informations soient fournies spontanément par le responsable du traitement aux personnes concernées[79]. L'idée est d'annoncer loyalement aux personnes concernées le sort qui attend leurs données et les éventuels risques encourus du fait du traitement de celles-ci. C'est parce que sa collecte de données sur des internautes non inscrits sur Facebook et navigant hors de ce réseau social fut jugée déloyale, que Facebook a été sanctionné tant en Belgique, par le tribunal civil de Bruxelles, qu'en France, par la CNIL[80] : « [c]oncernant la collecte des données de navigation des internautes, via le cookie "datr", l'information dispensée via le bandeau d'information relatif aux cookies est imprécise. En effet, cette mention ne fait qu'indiquer que des informations sont collectées "[...] sur et en

77 C. CADWALLADR et E. GRAHAM-HARRISON, « Revealed : 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach », 17 mars 2018, *The Guardian*, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election ; M. ROSENBERG, N. CONFESSORE et C. CADWALLADR, « How Trump Consultants Exploited the Facebook Data of Millions », 17 mars 2018, *The New York Times*, https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook ; CNIL, « Affaire Cambridge Analytica/Facebook », 12 avril 2018, https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook.

78 Voy. le considérant 60 du RGPD : « [l]e principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités ». Également : « [f]air processing means transparency of processing, especially vis-à-vis data subjects » (European Union Agency for Fundamental Right (FRA), European Court of human rights, Council of Europe, *Handbook on European data protection law*, 2014, p. 76, https://rm.coe.int/16806b294a). « Transparency is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the EU » (Groupe de l'Article 29, Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018, WP 260rev01, § 2).

79 Voy. les art. 13 et 14 du RGPD qui imposent un devoir d'information des personnes concernées, soit lors d'une collecte directe des données, soit lors d'une collecte indirecte. De même voy. l'art. 8 de la Convention 108+.

80 La condamnation prononcée se base sur les lois française et belge mettant en œuvre l'art. 6, § 1er, a), de la directive 95/46. Cette disposition étant reprise à l'art. 5, § 1er, a), du RGPD, on peut estimer que le raisonnement serait identique sous l'empire du RGPD. D'autres irrégularités au regard de la législation de protection des données étaient également reprochées à Facebook et ont été sanctionnées dans les deux décisions évoquées ici. Voy. délibération de la formation restreinte de la CNIL, SAN-2017-006, du 27 avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland. La sanction prononcée s'élève à 150.000 EUR, https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000034728338&fastReqId=390211096&fastPos=2 ; Trib. Civ. Bruxelles, 16 février 2018, n° de rôle 2016/153/A, https://www.privacycommission.be/sites/privacycommission/files/documents/jugement_facebook_16022018.pdf. Voy. également le communiqué de presse de la Commission belge de la protection de la vie privée, à l'adresse https://www.privacycommission.be/fr/news/victoire-de-la-commission-vie-privee-dans-la-procedure-facebook. E. DEGRAVE, « Facebook, les cookies et la justice belge : le retour », 22 mars 2018, *Justice en ligne*, http://www.justice-en-ligne.be/article1044.html ; A. CUSTERS et J. F. HENROTTE, « Le "cookie" "Datr" de Facebook : préservation de la sécurité des utilisateurs ou atteinte massive à la vie privée des internautes ? », *J.L.M.B.*, 2017, pp. 1249-1255.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



dehors de Facebook via les cookies", ce qui ne permet pas aux internautes d'être clairement informés et de comprendre que leurs données sont systématiquement collectées dès lors qu'ils naviguent sur un site tiers comportant un module social. Cette collecte massive de données effectuée via le cookie "datr" est déloyale en l'absence d'information claire et précise »[81].

La Cour de justice de l'UE a spécifié dans son arrêt dans l'affaire *Bara* que l'exigence de traitement loyal des données personnelles « oblige une administration publique à informer les personnes concernées de la transmission de ces données à une autre administration publique en vue de leur traitement par cette dernière en sa qualité de destinataire desdites données »[82]. L'information des personnes concernées à propos des transmissions de données effectuées entre administrations peut se faire par le biais de la norme sur la base de laquelle ont lieu ces transmissions. Mais il faut que cette norme soit suffisamment précise et explicite pour qu'on puisse considérer qu'elle réalise l'information exigée.

Le devoir d'informer activement les personnes concernées du traitement effectué sur leurs données vise à permettre à l'individu non seulement d'avoir connaissance, mais aussi de contrôler ce qui est fait avec ses données, de vérifier le respect des règles, de traquer les abus ou les illégalités, de corriger les erreurs[83]. Dans le monde d'Internet où l'opacité règne, l'information est la condition première de la prise de conscience de la réalité et de la capacité de contrôle tant des internautes dont les données et les traces sont récoltées au fil de leur navigation, que des personnes dont les données sont communiquées via le réseau.

Pour que ce droit à être informé ne soit pas un leurre, le RGPD exige que les informations à fournir le soient de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant[84]. Il est vrai que sous la directive 95/46, le responsable du traitement devait déjà communiquer aux personnes concernées toute une série d'informations mais celles-ci étaient rarement lues en raison notamment de la longueur et de la complexité des documents dans lesquels elles

81 CNIL, « Facebook sanctionné pour de nombreux manquements à la loi Informatique et Libertés », 16 mai 2017, https://www.cnil.fr/fr/facebook-sanctionne-pour-de-nombreux-manquements-la-loi-informatique-et-libertes.

82 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14, pt 34.

83 C.J.C.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, C-553-07, pt 54.

84 Art. 12, § 1, du RGPD.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



étaient insérées. Le législateur européen tente dès lors dans le RGPD de remédier à ce problème en mettant l'accent sur la transparence et la clarté avec lesquelles les informations doivent être mises à disposition. L'utilisation d'icônes[85], par exemple, devrait permettre de donner d'emblée aux individus une bonne visibilité sur le traitement.

Le droit à l'information n'est bien sûr pas absolu et une série d'exceptions peuvent intervenir au nom d'intérêts supérieurs comme la poursuite des infractions ou la protection du secret professionnel.

### C. – *Respect de l'attente raisonnable et du principe de finalité ; minimisation des données et limitation de leur conservation*

#### 1. – *Le respect de l'attente raisonnable et du principe de finalité*

Principe clé de la protection, le principe de finalité exige que tout traitement poursuive une ou des finalité(s) déterminée(s), explicite(s) et légitime(s), et que l'on ne fasse que ce qui est compatible avec cette (ces) finalité(s)[86].

La finalité du traitement des données doit donc être fixée et claire dès avant la mise en œuvre du traitement. Si ce sont des textes législatifs qui mettent en place les traitements de données, ils doivent prévoir explicitement la ou les finalités poursuivies. Ces finalités doivent être définies avec suffisamment de précision et ne peuvent être vagues ou trop larges. En outre, la finalité doit être légitime, ce qui signifie qu'elle ne peut induire une atteinte disproportionnée aux droits, libertés et intérêts en jeu, au nom des intérêts poursuivis par le responsable du traitement[87]. La notion de légitimité invite donc à un examen de proportionnalité. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées. Les intérêts en jeu à prendre en considération sont, bien sûr, ceux de la personne concernée par les données, mais sont aussi, le cas échéant, l'intérêt de la société dans son ensemble. En résumé, pour être légitime, une finalité ne peut causer un

85 Art. 12, § 7, du RGPD.

86 Art. 5, § 1er, b), du RGPD ; art. 5, § 4, b), de la Convention 108+. Pour un cas d'utilisation non compatible des données condamnée par la Cour européenne des droits de l'homme, voy. Cour eur. D.H., 27 août 1997, *M.S. c. Suède*.

87 M.-H. BOULANGER, C. DE TERWANGNE, Th. LÉONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 145 ; Th. LÉONARD et Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », in *La vie privée, une liberté parmi les autres ?* (F. RIGAUX), coll. Travaux de la Faculté de droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



préjudice plus grand à l'ensemble des intérêts en jeu que l'intérêt que représente le traitement[88]. On retrouve au niveau de la finalité la même exigence de proportionnalité que pour le traitement lui-même[89].

Le principe de finalité implique aussi que seules les utilisations compatibles avec la ou les finalités déterminées et annoncées au départ, au moment de la collecte, sont admises[90]. La notion d'utilisation « compatible » doit s'entendre en tenant compte des nécessités de transparence et de loyauté du traitement de données[91]. En particulier, les données à caractère personnel ne doivent pas faire l'objet d'un traitement ultérieur que la personne concernée pourrait considérer comme inattendu, inapproprié ou contestable[92].

Cet aspect du principe de finalité se retrouve également dans la jurisprudence de la Cour européenne des droits de l'homme. Dans l'affaire *M.S. c. Suède*[93], des données médicales confidentielles, personnelles et sensibles d'une patiente avaient été communiquées, sans le consentement de celle-ci, d'une autorité publique à une autre. Selon la Cour, « [l]a communication ultérieure servait un but différent » et « […] la divulgation des informations dépendait d'une série d'éléments dont la maîtrise échappait à l'intéressée »[94]. En conséquence, la Cour a estimé que la communication des données avait porté atteinte au droit au respect de la vie privée de la patiente. Pour que cette atteinte soit admissible, il faut que la communication des données puisse entrer dans les attentes raisonnables des intéressés. Dans le cas de communication réalisée en exécution d'une mission légale, comme dans l'affaire *M.S.*, il importe que

88 Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), 18 mai 2018, § 48 : « [l]a légitimité d'une finalité dépendra des circonstances, le but étant de garantir dans chaque cas un juste équilibre entre les droits, les libertés et les intérêts en jeu : le droit à la protection des données à caractère personnel, d'une part, et la protection d'autres droits, d'autre part. Un juste équilibre doit ainsi être ménagé entre les intérêts de la personne concernée et ceux du responsable du traitement ou de la société ». Voy. aussi la jurisprudence de la Cour européenne des droits de l'homme et celle de la Cour de justice de l'UE citées *supra*, pt III, A.

89 Voy. *supra*, III, A.

90 Art. 5, § 1er, b) et art. 6, § 4, du RGPD ; art. 5, § 4, b), de la Convention 108 modernisée. On notera que le RGPD admet le traitement ultérieur des données à des fins incompatibles avec ce qui était prévu au départ à la condition que ce traitement ultérieur s'appuie sur le consentement de la personne concernée ou qu'il soit basé sur le droit de l'Union ou d'un État membre visant à garantir un des objectifs énumérés à l'art. 23 du RGPD, c'est-à-dire, en particulier, « d'importants objectifs d'intérêt public général » (considérant 50 du RGPD) ; la norme juridique dont question doit constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir l'objectif visé (art. 6, § 4, du RGPD).

91 Rapport explicatif de la Convention 108+, préc., § 49.

92 *Ibid*. Le RGPD présente, à son art. 6, § 4, une série de critères – repris dans le rapport explicatif de la Convention 108 modernisée – permettant d'établir si la finalité du traitement à une autre fin est compatible ou non avec la finalité de la collecte de départ. Il s'agit du lien pouvant exister entre les deux finalités, du contexte, de la nature des données, des conséquences du traitement ultérieur et des garanties existantes.

93 Cour eur. D.H., 27 août 1997, *M.S. c. Suède*.

94 *Ibid.*, § 35.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



cette communication soit prévue par une norme accessible suffisamment précise[95].

### 2. – *Minimisation des données et limitation de leur conservation*

Deux exigences quant aux données sont directement liées au principe de finalité.

Tout d'abord celle que l'on ne conserve les données qu'aussi longtemps que cela est nécessaire pour atteindre la finalité du traitement[96]. Une fois que cela ne se justifie plus, il faut supprimer ou anonymiser les données.

Ensuite, l'exigence que l'on ne traite que des données pertinentes et non excessives[97] (ou limitées à ce qui est nécessaire[98]) par rapport aux finalités pour lesquelles elles ont été collectées. Le critère de nécessité s'exprime tant au niveau de la quantité des données que de leur qualité[99]. Ainsi, s'il est clair qu'on ne peut traiter un nombre excessif de données (par exemple demander à un employé l'ensemble de ses données médicales pour juger de son aptitude au travail), on ne peut davantage se lancer dans le traitement d'une seule donnée qui, même pertinente au vu de la finalité, porterait excessivement atteinte aux droits et intérêts de la personne concernée par rapport à l'intérêt qu'elle présente pour la personne qui souhaite la traiter.

C'est précisément la question du caractère excessif d'une donnée qui était au cœur de la retentissante affaire *Google Spain*[100]. Cette affaire a permis à la Cour de justice de l'UE de consacrer le droit au déréférencement sur Internet[101]. La Cour a en ce sens précisé qu'une personne concernée peut exiger que soient effacées les données qui la concernent

95 Pour une condamnation par la Cour européenne des droits de l'homme d'une transmission de données entre un service médical et une autorité administrative car cette transmission ne constituait pas une application prévisible de la législation en cause, voy. Cour eur. D.H., 23 février 2016, *Y.Y. c. Russie*.

96 Art. 5, § 1er, e), du RGPD ; art. 5, § 4, e), de la Convention 108+ ; Cour eur. D.H., 18 septembre 2014, *Brunet c. France*.

97 Art. 5, § 1er, c), du RGPD ; art. 5, § 4, c), de la Convention 108+ ; C.J.U.E., *Digital Rights*, préc., pts 56 à 59 ; Cour eur. D.H. (Gde ch.), 4 décembre 2008, *S. et Marper c. Royaume Uni*, § 103.

98 Art. 5, § 1, c), du RGPD.

99 Dans ce sens, voy. l'explication de la notion de données « excessives » dans le rapport explicatif de la Convention 108+ : « [c]ette disposition vise aussi bien les aspects quantitatifs que qualitatifs des données à caractère personnel. Des données qui seraient adéquates et pertinentes mais entraîneraient une ingérence disproportionnée dans les droits et libertés fondamentaux en jeu doivent être considérées comme excessives et ne pas être traitées ».

100 C.J.U.E., 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12. Voy. les références des commentaires doctrinaux de cette affaire mentionnées à la note 129.

101 Voy. la contribution d'Edouard Cruysmans dans le présent ouvrage, « La protection de la réputation en ligne : droit de réponse, droit de rectification, droit à l'oubli ».



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



en cas de non-respect de l'exigence de qualité des données. Selon la Cour, ce non-respect « peut résulter non seulement du fait que ces données sont inexactes, mais, en particulier, aussi du fait qu'elles sont inadéquates, non pertinentes ou excessives au regard des finalités du traitement, qu'elles ne sont pas mises à jour ou qu'elles sont conservées pendant une durée excédant celle nécessaire, à moins que leur conservation s'impose à des fins historiques, statistiques ou scientifiques »[102]. Cette qualité des données s'évalue au regard des finalités pour lesquelles les données sont traitées mais la Cour a ajouté que l'évaluation se fait également au regard de l'écoulement du temps[103]. Il se peut donc que des informations qui pouvaient passer pour pertinentes à un moment donné se révèlent ne plus l'être ou être devenues excessives par la suite, eu égard à l'ensemble des circonstances du cas considéré[104].

## IV. Droits accordés aux personnes concernées

Toute personne, quels que soient son âge, son domicile ou sa nationalité, se voit reconnaître des droits vis-à-vis des données la concernant qui font l'objet d'un traitement. Tant le RGPD que la version modernisée de la Convention 108 ont étoffé remarquablement la liste des droits garantis et ont renforcé ces derniers par rapport à ce qui existait auparavant. La jurisprudence des deux cours européennes est allée dans le sens d'une affirmation claire de droits pour les individus sur qui on collecte des données. Dans le cadre de la présente réflexion centrée sur Internet, on s'attardera sur les droits qui présentent un intérêt particulier dans ce contexte.

Le *droit à l'information* sur le traitement des données a déjà été évoqué ci-avant avec le devoir de loyauté (*cf.* point III, B). On ajoutera que ce droit ne va pas jusqu'à imposer aux médias ou à quiconque souhaite diffuser sur Internet des informations d'intérêt public relatives à une personne physique une obligation de notification préalable, qui conduirait à prévenir cette personne de ce qu'on compte publier sur elle. Cela serait inévitablement susceptible de constituer une forme de censure avant

102 *Ibid.*, § 92.
103 *Ibid.*, § 93.
104 C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », in *Les enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 264.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



la publication[105]. Par contre, la solution de consulter préalablement la personne concernée, voire même d'obtenir son consentement, avant de communiquer les informations la concernant peut être envisagée dans des circonstances où il ne s'agit pas de communication publique au nom de la liberté d'expression et du droit du public à l'information. La Cour européenne des droits de l'homme a ainsi évoqué cette solution dans l'affaire *Avilinka*, dans le cadre de transmission d'informations médicales confidentielles aux autorités publiques à propos de témoins de Jéhovah[106]. C'est aussi dans cette ligne que s'inscrit la législation de protection des données qui impose un devoir de transparence[107] vis-à-vis des personnes à propos de qui on récolte ou on communique des données, et qui requiert d'obtenir le consentement des individus[108] pour sortir des finalités poursuivies initialement. Tel était le cas dans l'affaire *Avilinka* tranchée par la Cour, dans laquelle on était passé d'un traitement de données dans un contexte médical à un traitement dans un contexte administratif ou policier.

Le *droit d'accès* permet à la personne concernée d'obtenir à sa demande – et non plus passivement, comme avec le droit à l'information – des informations sur les traitements effectués sur ses données[109]. Entre la première formulation du droit d'accès dans la Convention 108 et celle contenue dans la version modernisée de la Convention et dans le RGPD, une remarquable extension de ce droit est apparue. L'accès aujourd'hui ne se réduit plus à la seule connaissance de l'existence d'un fichier, de l'identité de son responsable et des données qu'il contient. L'accès s'exerce à l'égard de ces informations mais est une prérogative bien plus riche désormais. Selon la Cour de justice de l'Union européenne[110], le sens même du droit d'accès dans toutes ses composantes est de permettre aux individus de prendre connaissance du sort réservé à leurs données et de procéder à des vérifications des opérations effectuées sur elles, afin d'être à même d'exercer leurs autres droits prévus par la directive.

105 Cour eur. D.H., 10 mai 2011, *Mosley c. Royaume Uni*.
106 Cour eur. D.H., *Avilkina c. Russie*, préc., § 48.
107 Art. 13 et 14 du RGPD ; art. 8 de la Convention 108+. Voy. *supra*, III, B.
108 Ou de pouvoir s'appuyer sur une norme légale qui l'autorise (voy. art. 6.4 du RGPD).
109 Cour eur. D.H. (plén.), 7 juillet 1989, *Gaskin c. Royaume-Uni*, § 49 ; (Gde ch.), *Odièvre c. France*, §§ 41-47 ; 27 octobre 2009, *Haralambie c. Roumanie*, §§ 86-89 ; 7 décembre 2017, *Yonchev c. Bulgarie*, § 62.
110 C.J.C.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, C-553/07. Voy. C. GAYREL, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de justice de l'Union européenne, Tribunal de Première Instance et Tribunal de la Fonction publique européenne », *R.D.T.I.*, 2012, n$^{os}$ 48 et 49, pp. 95 et 96.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



La personne concernée qui apporte la preuve de son identité a le droit d'obtenir du responsable du traitement la communication, sous une forme claire et intelligible, des données faisant l'objet du traitement[111]. Le responsable du traitement doit fournir gratuitement[112] une copie des données[113]. C'est l'ensemble des données traitées qui doivent être communiquées, tant les données objectives que les données subjectives (par exemple, un avis, l'évaluation d'un employé, l'évaluation et les remarques émises par un examinateur[114]). La Cour européenne des droits de l'homme a relevé l'intérêt que représente le fait d'obtenir une copie des données : « [l]a Cour observe également que les intéressées ont considéré qu'il leur fallait disposer de tous les documents sous forme de photocopies afin qu'un expert indépendant, le cas échéant à l'étranger, puisse les examiner et aussi afin qu'elles puissent se prémunir contre une éventuelle destruction par mégarde des originaux »[115]. La Cour a aussi précisé que « l'intéressé ne doit pas être contraint de justifier spécifiquement la demande qu'il forme pour recevoir une copie de ces dossiers. C'est plutôt aux autorités qu'il revient de démontrer l'existence de raisons impérieuses de refuser un tel service »[116].

Le droit d'accès s'étend aux informations sur les destinataires ou les catégories de destinataires[117] à qui les données sont communiquées. Cette dimension du droit d'accès présente un intérêt certain dans le contexte d'Internet pour quiconque souhaite connaitre à qui, développeurs d'application, partenaires commerciaux ou autorités publiques, ses données ont été transmises. Ce droit peut prendre la forme d'une obligation pour le responsable du traitement de prendre l'initiative de l'information[118], ou d'un droit pour la personne concernée de recevoir cette information à sa demande[119].

Cette information à communiquer à propos des destinataires des données soulève la question de la portée dans le temps de ce type

111 Art. 15 du RGPD ; art. 9, § 1er, b), de la Convention 108+.
112 Art. 12, § 5, du RGPD ; Rapport explicatif de la Convention 108+, § 76.
113 Art. 15, § 3, du RGPD ; voy. pour l'accès à des copies d'examen : C.J.U.E., 20 décembre 2017, *Novak c. Data protection Commissioner*, C-434/16 ; concernant l'obtention de photocopies de dossiers médicaux, voy. Cour eur. D.H., 27 avril 2009, *K.H et autres c. Slovaquie*, § 47 : « [g]ardant à l'esprit que l'exercice du droit au respect de la vie privée et familiale, consacré par l'article 8, doit être concret et effectif, la Cour considère que pareilles obligations positives doivent s'étendre – en particulier dans les affaires qui comme l'espèce portent sur des données à caractère personnel – à la mise à disposition, en faveur de la personne concernée, de copies des dossiers dont elle est l'objet ».
114 C.J.U.E., 20 décembre 2017, *Novak c. Data protection Commissioner*, C-434/16, pts 42 et s.
115 Cour eur. D.H., *K.H. et autres c. Slovaquie*, préc., § 51.
116 *Ibid*., § 48.
117 Art. 13, § 1er, e), et art. 14, § 1er, e), du RGPD ; art. 8, § 1er, d), de la Convention 108+.
118 Art. 13 et 14 du RGPD ; art. 8, § 1er, de la Convention 108+.
119 Art. 15 du RGPD ; art. 9, § 2, de la Convention 108+.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



d'information. En effet, c'est souvent parce que l'on s'est rendu compte de quelque chose de douteux ou parce que l'on souhaite savoir à quelle source des personnes ont obtenu des informations, que l'on exerce son droit d'accès pour découvrir les personnes à qui les données ont été transmises. L'accès aux données sur les destinataires est, dans un monde numérisé, lié à la question de l'accès aux *log files* ou journaux d'événements. Ces derniers sont des fichiers qui relèvent un certain nombre de renseignements sur toutes les transactions gérées par le serveur. C'est donc à partir de ces journaux et des traces numériques qu'ils conservent que l'on peut identifier les accès qui se sont produits. L'information sur les destinataires se heurte toutefois directement aux pratiques d'effacement de telles données au terme d'un certain délai. La Cour de justice de l'Union européenne[120] a affirmé que le sens même du droit d'accès dans toutes ses composantes est de permettre aux individus de prendre connaissance du sort réservé à leurs données et de procéder à des vérifications des opérations effectuées sur elles, afin d'être à même d'exercer leurs autres droits prévus par la directive. En conséquence, pour la Cour, il est impératif que l'accès ne soit pas réduit au présent, mais couvre également le passé. Il ne s'agit pas pour autant de permettre de remonter sans limites dans le temps. La fixation d'un délai de conservation légitime varie en fonction de paramètres identifiés par la Cour et doit être tempérée par l'intervention du critère de proportionnalité[121]. L'arrêt *Rijkeboer* présente un enseignement concret pour les responsables de traitement. Ils savent à l'avenir que pèse sur eux l'obligation de veiller à la conservation des traces des communications et accès aux données accordés à des tiers au moins pendant une durée raisonnable, afin de permettre aux personnes concernées d'être informées de ces transmissions de leurs données et de pouvoir en contrôler la licéité.

La personne concernée a également le droit d'accès à la logique ou au raisonnement qui sous-tend le traitement des données[122] y compris les conséquences de ce raisonnement et les conclusions qui peuvent en avoir été tirées, en particulier lors de l'utilisation d'algorithmes pour une prise de décision automatisée, notamment dans le cadre du profilage[123].

120 C.J.C.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, C-553/07. Voy. C. GAYREL, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de justice de l'Union européenne, Tribunal de Première Instance et Tribunal de la Fonction publique européenne », *op. cit.*, pp. 95 et 96.

121 Voy. les pts 58, 59 et 63 de l'arrêt et leur commentaire dans C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 7 mai 2009, *R.D.T.I.*, 2011, n° 43, pp. 65 à 81.

122 Art. 15, § 1er, h), du RGPD ; art. 9, § 1er, c), de la Convention 108+.

123 Rapport explicatif de la Convention 108+, § 77.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



Ce droit présente un grand intérêt face au déploiement exponentiel du phénomène de profilage. Ce phénomène est particulièrement répandu sur Internet où il est utilisé dans le cadre du cybermarketing ou d'autres domaines d'activités pour analyser ou prédire des aspects de la vie de la personne concernée, comme « sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements »[124]. Il a été pris spécifiquement en considération par les auteurs du RGPD et de la Convention 108+ qui proclament le *droit de ne pas faire l'objet d'une décision ou d'une mesure* affectant un individu, impliquant l'évaluation de certains aspects personnels et *prise sur le seul fondement d'un traitement automatisé*[125]. Le recours au profilage est toutefois admis dans certaines circonstances, notamment s'il est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ou si la personne concernée a donné son consentement explicite, mais il doit alors être assorti de garanties comprenant le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision[126]. Le considérant 71 du RGPD précise encore que le profilage « ne devrait pas concerner un enfant », vœu qui est loin d'être réalisé dans le monde d'Internet.

La maitrise des données à caractère personnel implique de pouvoir vérifier le respect des règles de protection. En conséquence, outre le droit d'information et d'accès, l'individu concerné par les données se voit reconnaitre un *droit de rectification*[127] des données incorrectes et un *droit de faire effacer*[128] les données non pertinentes, celles portant excessivement atteinte à ses droits et intérêts, et celles conservées au-delà de la période autorisée. Ce droit à l'effacement est présenté, dans le RGPD, comme assimilé au *droit à l'oubli*, notion qui a fait couler beaucoup d'encre et suscité de nombreux débats[129]. La personne concernée

124 Considérant 71 du RGPD.
125 Art. 22 du RGPD ; art. 9, § 1er, a), de la Convention 108+.
126 Art. 22, §§ 2 et 3, et considérant 71, du RGPD ; rapport explicatif de la Convention 108+, § 75.
127 Art. 16 du RGPD ; art. 9, § 1er, e), de la Convention 108+.
128 Art. 17 du RGPD ; art. 9, § 1er, e), de la Convention 108+.
129 Voy. le retentissant arrêt C.J.U.E. (Gde ch.), 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12. Égal. Cour eur. D.H., 28 juin 2018, *M.L. et W.W. c. Allemagne* ; 13 novembre 2012, *M.M. c. Royaume-Uni*. En doctrine : J. AUSLOOS et B. VAN ALSENOY, « Bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens », *A & M*, 2014/5, p. 398 ; C. BERNARD-GLANZ, « Les arrêts *Digital Rights Ireland* et *Google Spain*, ou le printemps européen de la protection des données », *C.D.E.*, 2014/3, pp. 685-717 ; A. CASSART et J. HENROTTE, « Arrêt *Google Spain* : la révélation d'un droit à l'effacement plutôt que la création d'un droit à l'oubli », *J.L.M.B.*, 2014 ; E. CRUYSMANS et A. STROWEL, « Un droit à l'oubli face aux moteurs de recherche : droit applicable et responsabilité pour le référencement de données



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



dispose également du *droit de s'opposer*[130] aux utilisations non compatibles avec la finalité annoncée et aux communications et aux accès non autorisés. Pour pouvoir effectuer ces vérifications, il s'impose de conserver pendant un certain temps des traces des opérations réalisées sur les données[131].

Enfin, le RGPD garantit aux personnes concernées un nouveau droit : le *droit à la portabilité des données*[132]. Aux termes de l'article 20, en cas de traitement automatisé de données fondé sur un contrat ou sur le consentement de la personne concernée, cette dernière a le droit de recevoir du responsable du traitement les données à caractère personnel qu'elle a fournies, « dans un format structuré, couramment utilisé et lisible par machine », afin de transmettre ces données à un autre responsable du traitement. Lorsque cela est techniquement possible, le responsable du traitement devra transmettre lui-même, à la demande de la personne concernée, les données directement à un autre responsable du traitement[133]. La création de ce nouveau droit à la portabilité est liée à l'apparition des réseaux sociaux[134]. Elle témoigne « de la volonté claire d'éviter que les personnes concernées ne soient "coincées"[135] par les géants actuels tels que Facebook ou Google, en permettant à ces personnes de "porter" les données à caractère personnel qu'elles avaient fournies à ces géants vers un nouveau service alternatif en ligne. De fait, en l'absence d'un tel droit, l'on pourrait tout à fait imaginer que la personne concernée s'abstienne de faire usage d'un tel service alternatif, se résignant, par exemple, à rester "fidèle" à Facebook, au vu de l'investissement temporel substantiel que représenterait, pour cette personne concernée, le fait d'ajouter elle-même, sur ce nouveau service,

"inadéquates, non pertinentes ou excessives" », *J.T.*, 2014, p. 451 ; E. DEFREYNE et R. ROBERT, « L'arrêt "Google Spain" : une clarification de la responsabilité des moteurs de recherche… aux conséquences encore floues », *R.D.T.I.*, 2014/3, pp. 73-114 ; C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *Les enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 237-268 ; D. LINDSAY, « The "Right to be Forgotten" by Search Engines under Data Privacy Law : A Legal Analysis of the Costeja Ruling », *Journal of Media Law*, 2014/6, pp. 159-179. Voy. sur le sujet la contribution d'Edouard Cruysmans dans le présent ouvrage.

130 Art. 21 du RGPD ; art. 9, § 1er, d), de la Convention 108+.

131 Sur le devoir de conserver des traces pour vérifier les accès accordés aux données, voy. Cour eur. D.H., 17 juillet 2008, *I. c. Finlande* ; C.J.C.E., 7 mai 2009, *Rijkeboer*, C-553-07.

132 Voy. Groupe de l'Article 29, Guidelines on the Right to Data Portability, 13 avril 2017, WP 242 rev.01.

133 Art. 20, § 2, du RGPD.

134 D. DE BOT, « De uitvoering van de algemene verordening gegevensbescherming – enkele bemerkingen bij de Belgische context », *T.V.W.*, 2016/3, p. 221.

135 « *Lock-in* ».



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



l'ensemble des données à caractère personnel qu'elle aurait déjà "*uploadé*" sur Facebook (informations personnelles, photos, etc.) »[136].

Dans la ligne de l'apparition de ce droit à la portabilité, est né en 2017 le « *Data Transfer Project* »[137], fruit d'une collaboration entre Google, Facebook, Microsoft et Twitter. Ce projet œuvre à la création d'une plateforme open-source en vue d'assurer concrètement la portabilité directe des données entre les fournisseurs de services participants.

## V. Obligation de sécurité

Le devoir de sécurité des données figure désormais au rang des principes de base de la protection des données[138], devoir classique mais ô combien crucial aujourd'hui où les données à caractère personnel représentent un eldorado attisant les convoitises des cyber-criminels en tout genre[139].

Le responsable du traitement doit protéger les données à caractère personnel qu'il a collectées contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées, qu'elles soient de nature accidentelle ou malintentionnées[140].

Les mesures de sécurité à prendre sont de deux ordres : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, utiliser des mots de passe renouvelés régulièrement, fermer les locaux où sont localisés les ordinateurs et les fichiers, etc.) et des mesures techniques (programme anti-virus fréquemment mis à jour, *firewalls*, *backup* de sécurité, *login*...).

136 Th. TOMBAL, « Les droits de la personne concernée dans le RGPD », in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie* (C. DE TERWANGNE et K. ROSIER dir.), Bruxelles, Larcier, 2018, p. 484.

137 https://datatransferproject.dev/.

138 Art. 5, § 1er, f), et 32 du RGPD ; art. 7 de la Convention 108+ et les §§ 62 à 66 du rapport explicatif de la Convention 108+. Cour eur. D.H., 17 juillet 2008, *I. c. Finlande*.

139 En ce sens, voy. European Commission, Joint communication to the European Parliament and the Council, « Resilience, Deterrence and Defence : Building strong cybersecurity for the EU », 13 septembre 2017, JOIN (2017) 450 final ; McAfee & Centre for Strategic and International Studies, *Net losses: Estimating the Global Cost of Cybercrime*, 2014, https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrimef ; EUROPOL, *Serious and Organised Crime Threat Assessment*, 2017, https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment.

140 C.J.U.E., *Digital Rights*, pt 66 : « [d]e surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive 2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données » ; pt 67 : « […] En particulier, la directive 2006/24 ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci ».



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



Elles doivent assurer un niveau de protection approprié, adapté au risque que présente le traitement en question et tenant compte de différents facteurs[141]. Ainsi, plus les données en cause sont sensibles et les risques pour la personne concernée élevés, plus importantes seront les précautions à prendre. Par exemple, des données génétiques utilisées en dehors d'un contexte médical (par exemple, par une entreprise offrant via Internet un service d'identification des liens d'ascendance/descendance par analyse génétique), doivent être encadrées de mesures de sécurité sévères.

Cela étant, aucun responsable de traitement n'est à l'abri d'une faille de sécurité, les *hackers* faisant sans cesse preuve d'inventivité pour pénétrer les systèmes informatiques. De telles failles de sécurité peuvent entraîner la perte, l'altération ou la divulgation de données personnelles et être préjudiciables pour l'individu ou pour le responsable du traitement. Tant le RGPD[142] que la Convention 108+[143] prévoient désormais une obligation de notifier à l'autorité de contrôle, voire aux personnes concernées, les violations de données susceptibles de porter gravement atteinte aux droits et libertés fondamentaux de la personne concernée. C'est le cas, par exemple, lors de la révélation de données couvertes par le secret professionnel, ou susceptibles d'entraîner un préjudice financier, une atteinte à la réputation, des dommages corporels ou une humiliation[144].

## VI. Protection des données en conflit avec d'autres libertés ou droits fondamentaux sur Internet

Dans le contexte d'Internet, la protection des données à caractère personnel risque d'entrer en conflit avec d'autres droits et libertés.

### A. – *Conflit avec la propriété intellectuelle*

Il peut, par exemple, s'agir d'un conflit avec le droit de propriété intellectuelle[145], illustré notamment par l'affaire *Promusicae*[146] qui a vu la Cour de justice de l'Union européenne établir que les États peuvent – sans

141 Voy. l'art. 32 du RGPD et le § 62 du rapport explicatif de la Convention 108+.
142 Art. 33 et 34 du RGPD.
143 Art. 7, § 2, de la Convention 108+.
144 § 64 du rapport explicatif de la Convention 108+. Voy. égal. les considérants 85 et 96 du RGPD.
145 Voy. sur ce point la contribution de Benoît Michaux dans le présent ouvrage.
146 C.J.C.E. (Gde ch.), 29 janvier 2008, *Promusicae c. Telefonica de Espana SAU*, C-275/06.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



y être obligés – prévoir des limitations à la protection des données au nom de la protection d'autres droits d'autrui comme le droit de propriété et le droit à un recours effectif[147]. Les États peuvent donc autoriser la transmission par les fournisseurs de services de communications électroniques des adresses IP aux sociétés d'auteurs gardiennes de la protection des droits de propriété intellectuelle de leurs affiliés.

### B. – *Conflit avec la liberté d'expression et d'information*

La protection des données doit être conciliée avec les impératifs de protection de la liberté d'expression et d'information.

Le préambule de la Convention 108 modernisée le rappelle explicitement : « [r]appelant que le droit à la protection des données à caractère personnel est à considérer au regard de son rôle dans la société et qu'il est à concilier avec d'autres droits de l'homme et libertés fondamentales, dont la liberté d'expression »[148]. La Convention se veut donc l'expression de cette conciliation. L'article 11 autorisant certaines exceptions au régime de protection (touchant principalement aux conditions de légitimité des traitement et de qualité des données, ainsi qu'aux droits des personnes concernées) prévoit qu'une exception est admise si, prévue par la loi, elle respecte l'essence des droits et libertés fondamentales et constitue une mesure nécessaire et proportionnée dans une société démocratique à la protection de la personne concernée ou des droits et libertés fondamentales d'autrui, notamment la liberté d'expression. L'article 14 réglant le sort des flux transfrontières admet aussi qu'un transfert de données ait lieu sans tenir compte des exigences habituelles, si ce transfert « constitue une mesure nécessaire et proportionnée dans une société démocratique pour la liberté d'expression ».

Le RGPD, quant à lui, bien qu'offrant un régime dérogatoire dans la même ligne que la Convention n° 108+[149], invite expressément les États à concilier, dans leur loi nationale, le droit à la protection des données à caractère personnel « et le droit à la liberté d'expression et d'information,

147 Pour un cas de régime de limitation acceptable, voy. l'analyse du droit suédois faite par la Cour de justice dans l'affaire *Bonnier* : C.J.U.E., 19 avril 2012, *Bonnier e.a. c. Perfect Communication Sweden*, C-461/10.

148 4e alinéa du préambule de la Convention 108+.

149 L'art. 23, § 1er, i), du RGPD permet aux États membres de prévoir des exceptions aux principes, obligations et droits lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la protection des droits et libertés d'autrui (parmi lesquels la liberté d'expression).



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire »[150].

La notion de « traitement de données à caractère personnel effectué à des fins journalistiques » a très tôt suscité des difficultés. *A priori* limpide au temps de l'adoption de la directive 95/46, cette notion a perdu de sa clarté une fois placée dans le contexte d'Internet, et des interrogations concernant sa portée et son contour précis dans ce nouvel environnement se sont rapidement fait jour. Cette notion n'est en effet pas centrée sur un acteur (les médias) mais sur une activité (le journalisme). Or, on a dû constater que dans la sphère internet cette activité n'était plus l'apanage d'organes de presse bien établis et reconnus comme tels ou de journalistes patentés détenteurs d'une carte de presse. Peu à peu se sont développés des sites Web d'organisations et d'associations désireuses de mettre en lumière certaines informations ou de réagir à certaines actualités[151]. De même, des blogs personnels sont apparus par lesquels des individus publient à leur tour des informations qu'ils assortissent de commentaires personnels et qu'ils partagent avec un public invité à manifester ses réactions. Aujourd'hui, les réseaux sociaux et les forums ont également pris le relais dans la diffusion d'informations et c'est via Facebook, Twitter ou Youtube, par exemple, que certains, professionnels ou quidams, éminents spécialistes ou simples témoins, diffusent désormais dans le public des informations, des commentaires, des vidéos ou des photos liées à l'actualité.

Dans quelle mesure toutes ces hypothèses doivent-elles être comprises comme étant des activités poursuivant des « fins de journalisme » ? La question est d'autant plus pertinente que l'article 85 du RGPD réserve un sort particulièrement favorable aux traitements de données à caractère personnel qui poursuivent pareilles fins. Au nom de l'équilibre à trouver entre la protection des droits fondamentaux des personnes sur qui des données sont collectées et la liberté d'expression et de la presse, le RGPD invite les États membres à prévoir toutes les dérogations aux règles de protection des données (sauf celles se rapportant à

150 Art. 85 du RGPD. Pour un commentaire de ces nouvelles dispositions, voy. Q. VAN ENIS, « La conciliation entre le droit à la liberté d'expression et le droit à la protection des données à caractère personnel dans le RGDP », in *Le Règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie* (C. de Terwangne et K. Rosier dir.), coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 763-795.

151 La Cour européenne des droits de l'homme a élargi la protection accordée à la presse à ceux qui « font œuvre de presse ». Voy. not. Cour eur. DH, 27 mai 2004, *Vides Aizsardzības Klubs c. Lettonie*, § 42 : « [e]n tant qu'organisation non gouvernementale spécialisée en la matière, la requérante a donc exercé son rôle de "chien de garde" […]. Une telle participation d'une association étant essentielle pour une société démocratique, la Cour estime qu'elle est similaire au rôle de la presse tel que défini par sa jurisprudence constante » ou encore Cour eur. D.H., 15 février 2005, *Steel et Morris c. Royaume-Uni*, § 89.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



la responsabilité et aux voies de recours) qui s'avèrent nécessaires pour réaliser cet équilibre. Cet équilibre étant fort dépendant du contexte culturel, il a été jugé préférable par les auteurs du RGPD de laisser les États membres le définir, malgré la volonté d'uniformisation démontrée par l'adoption d'un règlement européen plutôt qu'une directive.

L'affaire *Linqvist* tranchée par la Cour de justice des Communautés européennes[152] a été la première au niveau de l'Union européenne à illustrer le propos. Peut-on sur Internet évoquer ses relations personnelles, associatives ou professionnelles sans devoir se soumettre aux exigences des règles de protection des données à caractère personnel ? La Cour a rappelé le devoir, compte tenu des circonstances, d'apprécier la proportionnalité de la restriction qui est apportée à l'exercice de la liberté d'expression du fait de l'application de règles visant à la protection des droits d'autrui.

À l'occasion de l'affaire *Satamedia*[153], la Cour de justice a mis en évidence la nécessité d'une approche stricte des dérogations à la protection. Cette affaire mettait en jeu un conflit entre la liberté d'expression (au bénéfice d'une société commerciale ayant développé un service de mise à disposition électronique d'informations fiscales sur les revenus patrimoniaux individualisés) et la protection de la vie privée (des personnes qui voyaient leurs données patrimoniales rendues publiques). La Cour a précisé à cette occasion qu'il fallait interpréter les notions afférentes à la liberté d'expression de manière large, mais « pour obtenir une pondération équilibrée entre les deux droits fondamentaux, la protection du droit fondamental à la vie privée exige que les dérogations et limitations de la protection des données prévues aux chapitres susmentionnés de la directive doivent s'opérer dans les limites du strict nécessaire »[154]. Quant à la détermination de la notion de journalisme, la Cour a affirmé qu'« il découle de tout ce qui précède que des activités […] peuvent être qualifiées d'"activités de journalisme", si elles ont pour finalité la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que ce soit. Elles ne sont pas réservées aux entreprises de

152 C.J.C.E., 6 novembre 2003, *Lindqvist*, C-101-01, *Rec.*, p. I-12971, §§ 43 et 44. Voy. C. DE TERWANGNE, « Arrêt *Lindqvist* ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », *R.D.T.I.*, 2004, n° 19, pp. 67 et s.

153 C.J.C.E., 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan markkinapörssi Oy et Satamedia Oy*, C-73/07.

154 C.J.C.E., 16 décembre 2008, *Satamedia*, préc., pt 56. Voy. C. DE TERWANGNE, « Les dérogations à la protection des données en faveur des activités de journalisme enfin élucidées », note sous C.J.C.E. (gde ch.), 16 décembre 2008, *Satakunnan Markkinapörssi Oy et Satamedia Oy*, aff. C-73/07, *R.D.T.I.*, 2010, n° 38, pp. 132-146.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



média et peuvent être liées à un but lucratif »[155]. C'est donc le seul fait que des activités visent la communication au public qui est décisif pour qualifier les activités de « journalistiques », ce qui est particulièrement large. On ne voit pas vraiment ce qui différencie cette définition de l'exercice de la liberté d'expression pure et simple.

Dans le régime général de la presse, si des droits spécifiques sont accordés aux « journalistes », c'est afin de leur permettre d'exercer sereinement et efficacement leur rôle qui consiste à communiquer des informations et des idées sur toutes les questions d'intérêt public[156]. Il en est ainsi par exemple du droit au secret des sources journalistiques. En contrepartie de ces droits, les bénéficiaires ont des devoirs. Les journalistes professionnels sont soumis à un code de déontologie garantissant notamment que la qualité des données recueillies et diffusées soit très sérieusement contrôlée. La Cour européenne des droits de l'homme a mis en exergue ce lien entre droits et obligations de ceux qui font œuvre de presse. Le respect des obligations déontologiques est présenté comme condition pour bénéficier des privilèges de la fonction. Ainsi, dans l'affaire relative au Canard enchaîné qui mettait en jeu la condamnation de journalistes pour recel de document obtenu en violation du secret professionnel, la Cour a spécifié : « [l]'article 10 protège le droit des journalistes de communiquer des informations sur des questions d'intérêt général dès lors qu'ils s'expriment de bonne foi, sur la base de faits exacts et fournissent des informations "fiables et précises" dans le respect de l'éthique journalistique »[157]. Il est donc interpelant que, dans son arrêt *Satamedia*, la Cour de justice fasse bénéficier toute personne qui s'exprime publiquement ou diffuse des informations dans le public du régime très protégé de la presse, régime normalement justifié par le rôle de celle-ci et conditionné au respect des règles de déontologie journalistique.

Les juridictions finlandaises interdirent toutefois aux sociétés concernées dans l'affaire *Satamedia* de poursuivre la publication massive des données fiscales. Aussi, celles-ci portèrent l'affaire devant la Cour européenne des droits de l'homme qui, à son tour, eut à se prononcer sur ce

155 § 61 de l'arrêt.

156 Conclusions de l'avocat général Mme Juliane Kokott du 8 mai 2008 dans l'affaire *Satakunnan Markkinapörssi Oy et Satamedia Oy*, C-73/07, pt 66 et les références citées des arrêts de la Cour européenne des droits de l'homme en ce sens.

157 Cour eur. D.H. (Gde ch.), 21 janvier 1999, *Fressoz and Roire v. France*, § 54. Dans le même sens, Cour eur. D.H., 15 décembre 2009, *Financial Times e.a. c. Royaume-Uni*, § 62 : « *Article 10 protects a journalist's right – and duty – to impart information on matters of public interest provided that he is acting in good faith in order to provide accurate and reliable information in accordance with the ethics of journalism* ».



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



conflit entre liberté d'expression des sociétés vendant les données fiscales et protection des données et de la vie privée des contribuables. La Cour[158] souscrit à la conclusion de la Cour administrative suprême finlandaise suivant laquelle la publication des données fiscales selon les modalités et à l'échelle en question n'avait pas contribué à un débat d'intérêt général. Dès lors, les sociétés requérantes ne pouvaient pas prétendre que cette activité de publication avait été exercée aux seules fins de journalisme. Pour vérifier si un juste équilibre a été atteint entre les intérêts concurrents, la Cour européenne des droits de l'homme s'est appuyée sur la série de critères déjà mis au jour par sa jurisprudence : « la contribution à un débat d'intérêt général, la notoriété de la personne visée, l'objet du reportage, le comportement antérieur de la personne concernée, le contenu, la forme et les répercussions de la publication, ainsi que, le cas échéant, les circonstances de la prise des photographies. Dans le cadre d'une requête introduite sous l'angle de l'article 10, la Cour vérifie en outre le mode d'obtention des informations et leur véracité ainsi que la gravité de la sanction imposée aux journalistes ou aux éditeurs »[159]. La Grande chambre a estimé qu'il n'y avait pas eu violation de la liberté d'expression des sociétés en cause.

Il est intéressant de relever qu'alors que la publicité des données fiscales en cause est organisée par la loi en Finlande où elle est acceptée socialement et s'appuie originellement sur une diffusion dans des journaux papier, la mise en place de services électroniques exploitant cette publicité et lui donnant une dimension tout autre[160] a vraisemblablement rompu l'équilibre de valeurs atteint auparavant et a

158 Cour eur. D.H. (Gde ch.), 27 juin 2017, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, § 165. Voy. Q. VAN ENIS, « Protection des données et liberté d'expression : (re)diffusion de données publiques ne rime pas (toujours) avec activités journalistiques, obs. sous Cour eur. dr. h., Gde ch., arrêt *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, 27 juin 2017 », *Rev. trim. D.H.*, 2018, vol. 116, pp. 953-984 ; D. VOORHOOF, « No Journalism Exception for Massive Exposure of Personal Taxation Dat », *Strasbourg Observers*, 5 juillet 2017.

159 Cour eur. D.H. (Gde ch.), 27 juin 2017, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, § 165.

160 *Ibid*, §§ 189 et 190 : « 189. Si les données fiscales en question étaient accessibles au public en Finlande, elles pouvaient être consultées uniquement dans les centres locaux des impôts et la consultation était soumise à des conditions claires. Il était interdit de copier ces informations sur des clés USB. Les journalistes pouvaient recevoir des données fiscales sous forme numérique, mais pareille extraction était également soumise à des conditions, et des limites étaient posées à la quantité de données pouvant faire l'objet d'une telle opération. Les journalistes devaient préciser que les informations étaient demandées à des fins de journalisme et qu'elles ne seraient pas publiées sous forme de listes. Dès lors, les informations relatives à des personnes physiques étaient certes accessibles au public, mais des règles et des garanties bien spécifiques s'appliquaient.
190. L'accessibilité des données en question au public en vertu du droit interne ne signifie pas nécessairement qu'elles pouvaient être publiées sans aucune restriction (paragraphes 48 et 54 ci-dessus). La publication des données dans un magazine et leur diffusion ultérieure au moyen d'un service de SMS *les ont rendues accessibles selon des modalités et à une échelle qui n'étaient pas prévues par le législateur* » (nos italiques).



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



conduit au rejet de cette voie de diffusion des données fiscales par les plaignants et, *in fine*, par la Cour administrative suprême finlandaise. Cet épisode judiciaire illustre la prudence qu'il faut avoir lorsqu'on envisage de « moderniser » des services de mise à disposition ou de diffusion d'informations en les faisant basculer d'un support classique (imprimé ou autre) vers Internet ou des applications numériques. Un tel basculement induit inévitablement le besoin de reconsidérer l'équilibre atteint jusque-là entre les droits et intérêts sacrifiés au bénéfice d'autres valeurs. Ce sain exercice conduira éventuellement à apporter les ajustements qui rétabliront l'équilibre rompu (anonymisation des données, accès réduit aux personnes justifiant d'un intérêt...).

En illustration de cette nécessaire reconsidération, la diffusion de la jurisprudence dans des bases de données désormais connectées au Web plutôt que dans des revues papier a dû être accompagnée d'une réflexion sur la nécessité d'anonymiser les décisions de justice rendues accessibles par ce biais, alors que la diffusion papier de ces mêmes décisions ne s'embarrassait pas de ce souci jusqu'alors. La portée d'une diffusion sur support papier est inévitablement plus restreinte, demande une démarche (aller dans une bibliothèque, par exemple), ne permet pas facilement les comparaisons, croisements et compilations de données. Ces caractéristiques sont parfois la clé de l'équilibre trouvé entre besoin d'information du public et protection des individus concernés.

## VII. Internet, instrument de surveillance, face à la protection des données

### A. – *Surveillance des données de connexion et de communication*

L'individu connecté laisse une série de traces de son passage et de ses actions sur le Web (adresse IP, fournisseur d'accès, page d'où il vient, historique de la navigation…) qui nourrissent, comme jamais aucune société totalitaire n'aurait osé le rêver, un potentiel de surveillance d'une finesse, omniprésence et permanence inégalées.

Par ailleurs, sur les réseaux sociaux, l'individu fournit lui-même à ses « amis », aux amis de ceux-ci voire au monde entier selon la configuration du réseau social employé, des informations qu'on aurait sans doute eu du mal à lui extorquer dans un commissariat de police. État d'esprit du matin, évocation des activités au bureau et à la maison, photos de vacances, de week-ends, de soirées, de plats de restaurant et de



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



vêtements achetés, commentaires sur le patron, sur les amis, annonces de mise en couple et de ruptures, les réseaux sociaux sont la version moderne du carnet intime qui n'est plus un carnet et n'a plus rien d'intime. Cette exposition de soi peut aussi être le fait de parents, d'amis ou de tiers plus ou moins bienveillants[161].

Cette transparence des individus connectés, qu'elle soit insoupçonnée ou assumée, interpelle et soulève la question de l'acceptabilité de la société de surveillance qui est en passe d'être édifiée. Cette interpellation a reçu un écho dans le prétoire des deux cours européennes. La Cour de justice tout comme la Cour européenne des droits de l'homme n'ont pas hésité à s'élever en rempart contre les excès de la surveillance électronique et spécialement de la surveillance de masse.

Sur Internet comme ailleurs, les personnes sont protégées contre les interceptions de leurs informations et communications, que ces interceptions soient le fait des autorités publiques[162] ou d'acteurs du secteur privé, comme les employeurs[163].

C'est dans un premier temps contre les agissements des autorités publiques que l'on veut garantir la confidentialité des échanges entre individus. Tant la jurisprudence[164] que les textes légaux[165] européens ont clarifié

161 Voy. J. ENRIQUEZ, « Déjà tatoué ? », UNICEF, *Les enfants dans un monde numérique*, décembre 2017, https://www.unicef.org/french/publications/files/SOWC_2017_FR.pdf : « Une fois adultes, les enfants et les adolescents d'aujourd'hui devront compter avec une surveillance et des antécédents qui dépassent l'imagination. Si la plupart d'entre nous avons eu la chance de pouvoir oublier, repenser ou réinventer une partie de notre vie, de nos amours, de nos emplois, de nos pensées, de nos actions, de nos commentaires et de nos erreurs du passé, les enfants de la génération actuelle se trouveront dans une position bien différente. [...] Qu'il le veuille ou non, chaque enfant aujourd'hui est [...] soumis à une scrutation qui n'a jamais été aussi puissante et permanente. Dès l'état de fœtus, lorsque leurs parents partagent échographies, voire séquences génétiques, ces enfants se voient tatouer publiquement des pans de leur vie. Avant même qu'ils n'entrent dans l'adolescence et commencent à partager eux-mêmes leurs histoires, ils portent déjà un grand tatouage qui peut définir la façon dont ils sont perçus. Où vis-tu ? Tes parents sont-ils divorcés ? D'ailleurs, qui sont-ils ? Quelle école as-tu fréquentée ? À quoi ressemblais-tu ? Quel sport pratiquais-tu ? Autant de questions auxquelles il est très facile de répondre ».

162 Parmi de nombreux arrêts, voy. Cour eur. D.H., 2 août 1984, *Malone c. Royaume Uni* ; 13 septembre 2018, *Big Brother Watch and Others c. Royaume-Uni*.

163 Voy. not. Cour eur. D.H., 3 avril 2007, *Copland c. Royaume Uni* ; (Gde ch.), 5 septembre 2017, *Barbulescu c. Roumanie*.

164 Cour eur. D.H., 25 septembre 2001, *P.G. et J.H. c. Royaume-Uni*, § 42 ; C.J.U.E. (Gde ch.), 8 avril 2014, *Digital Right Ireland*, aff. jointes C-293/12 et C-594/12. Voy. également Cour eur. D.H., 20 octobre 2015, *Sher et autres c. Royaume-Uni*, spéc. § 170 : « [l]es observations du tiers intervenant, Privacy International, portent essentiellement sur la perquisition d'appareils électroniques, pratique qui implique l'accès aux données personnelles et aux données de communication. Le tiers intervenant explique que les innovations technologiques offrent des possibilités de collecte, de stockage, de partage et d'analyse de données inimaginables auparavant. Selon lui, le contrôle par les forces de l'ordre des appareils électroniques d'un individu leur permet d'accéder à toutes les traces numériques laissées par celui-ci à quelque moment que ce soit, y compris les informations qui ne sont pas stockées sur ces appareils eux-mêmes mais sur des serveurs informatiques distants interconnectés. Le croisement de ces données serait extrêmement révélateur. La perquisition d'appareils électroniques revêtirait un caractère particulièrement intrusif, ce qui commanderait la fixation d'un seuil élevé d'exigence pour l'appréciation de la justification d'une atteinte aux droits protégés par l'article 8 ».

165 L'art. 5.1 de la directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « Vie privée et communications électroniques »), prescrit la confidentialité des communications ainsi que la confidentialité des



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



que la confidentialité doit porter sur le contenu des messages échangés mais également sur les données de communication (nom de l'émetteur, du destinataire, moment de la communication, longueur, numéro appelé ou, dans le cadre de communication via Internet, adresse IP, etc.).

Toute forme de surveillance n'est pas bannie pour autant. Les interceptions ne sont toutefois admises qu'au prix de strictes conditions protégeant la société contre les dérives de la surveillance étatique[166]. La Cour de justice de l'UE[167] a clarifié que, même des infractions pénales qui ne sont pas d'une particulière gravité peuvent justifier un accès par les autorités aux données à caractère personnel conservées par des fournisseurs de services de communications électroniques lorsque cet accès ne porte pas une atteinte grave à la vie privée. C'est le cas, par exemple, lorsque les données en question concernent l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et adresse de ces titulaires. Pour la Cour de justice, même si l'accès des autorités publiques à ces données représente une ingérence dans les droits fondamentaux des titulaires de cartes, cette ingérence ne saurait être qualifié de « grave » puisque ces données ne permettent pas de tirer de conclusions précises concernant la vie privée des individus concernés. Un tel accès ne devrait donc pas être limité aux cas de lutte contre la criminalité grave[168].

### B. – *Surveillance massive des communications*

Les données de communications (et non le contenu des communications) ont été pendant huit ans la cible d'une obligation de conservation systématique instaurée par la directive européenne 2006/24 du 15 mars 2006[169] et pesant sur les fournisseurs de services de communications électroniques accessibles au public et les fournisseurs de réseau public

données relatives au trafic y afférentes, c'est-à-dire toutes les données traitées en vue de l'acheminement d'une communication ou de sa facturation.

166 « La Cour estime que la loi dont la police s'est prévalue pour obtenir des informations sur l'abonné liées à l'adresse IP dynamique manquait de clarté et n'offrait pas de garanties suffisantes contre une ingérence arbitraire dans l'exercice des droits du requérant découlant de l'article 8 » (Cour eur. D.H., 24 avril 2018, *Benedik c. Slovénie*). Sur les garanties que doit présenter toute loi autorisant des interceptions, voy. Cour eur. D.H. (Gde ch.), 2 août 1984, *Malone c. Royaume-Uni* ; (Gde ch.), 16 février 2000, *Amann c. Suisse* ; (Gde ch.), 4 décembre 2015, *Roman Zakharov c. Russie* ; (Gde ch.), 12 janvier 2016, *Szabo et Vissy c. Hongrie* ; *Big Brother Watch and Others c. Royaume-Uni*, préc.

167 C.J.U.E. (Gde ch.), 2 octobre 2018, *Ministerio Fiscal*, C-2017/16.

168 *Ibid*., pt 61.

169 Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, *J.O.U.E.*, L 105, p. 54.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



de communications[170]. Cette obligation visait à garantir la disponibilité de ces données de communication au bénéfice des autorités publiques afin de leur permettre de mener des investigations en vue de la détection et de la poursuite d'infractions graves. La Cour de justice de l'Union européenne a estimé que, si l'ingérence répondait bien à un objectif d'intérêt général, à savoir contribuer à la lutte contre les infractions graves et le terrorisme, elle ne satisfaisait cependant pas l'exigence de proportionnalité. Pour la Cour de justice, la directive entraînait une ingérence d'une trop vaste ampleur et d'une gravité particulière dans les droits fondamentaux à la vie privée et à la protection des données personnelles consacrés par les articles 7 et 8 de la Charte des droits fondamentaux de l'UE, sans que des garanties encadrent une telle ingérence, assurant que celle-ci demeure limitée au strict nécessaire. La Cour a en conséquence invalidé la directive 2006/24 dans un arrêt retentissant[171].

Dans son non moins fracassant arrêt *Schrems*[172] qui la verra mettre un terme au *Safe Harbor*, système permettant les échanges de données avec les États-Unis, la Cour affirmera qu'« une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte ». Elle confirmera sa condamnation de la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation dans son arrêt *Tele2 Sverige* du 21 décembre 2016[173], tout en reconnaissant aux États le droit de prévoir, à titre préventif, une conservation *ciblée* de ces données pour lutter contre la criminalité grave, à condition qu'une telle conservation soit limitée au strict nécessaire[174].

170 Art. 3 de la directive 2006/24/CE, préc.

171 C.J.U.E. (Gde ch.), 8 avril 2014, *Digital Right Ireland*, aff. jointes C-293/12 et C-594/12, pts 69 et 71. Voy. F. DUBUISSON, « La Cour européenne des droits de l'homme et la surveillance de masse », *Rev. trim. D.H.*, 2016, pp. 870 et s. ; J.-P. FOEGLE, « Chronique du droit "post-Snowden" : la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme sonnent le glas de la surveillance de masse », *La Revue des droits de l'homme*, http://revdh.revues.org/2074.

172 C.J.U.E. (Gde ch.), 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, C-362/14, pt 94. Voy. C. DE TERWANGNE et C. GAYREL, « Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt *Schrems* », *Cahiers de Droit Européen*, 2017/1, pp. 35-81.

173 C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsenet Secretary of State for the Home Department/Tom Watson e.a.*, aff. jointes C-698/15 et C-203/15,

174 Ce qui fera dire à E. Wéry : « [l]e moins que l'on puisse dire, c'est que la Cour a de la suite dans les idées. Elle a placé la protection des données personnelles au panthéon des valeurs défendues par le droit de l'Union, et elle ne semble pas prête à modifier ce hit-parade » (https://www.droit-technologie.org/actualites/etats-ne-peuvent-imposer-obligation-generale-de-conservation-de-donnees/).



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



La Cour européenne des droits de l'homme s'est, elle aussi, insurgée contre la surveillance de masse. Elle n'a toutefois pas condamné l'interception massive des communications en tant que telle, comme la Cour de justice. Dans ses arrêts *Szabo et Vissy*[175], *Centrum for rädvisa*[176], et *Big Brother Watch*[177], la Cour a reconnu aux États une certaine latitude quant aux mesures à prendre pour assurer la sécurité nationale, au vu des menaces liées au terrorisme international et à la criminalité transfrontière. Parmi ces mesures, la Cour a accepté le recours à des technologies de pointe, notamment à des techniques de surveillance massive des communications, mais à certaines conditions strictes qu'elle avait déjà énoncées en présence de techniques d'écoutes téléphoniques. Ces conditions concernent « l'accessibilité du droit interne, la portée et la durée des mesures de surveillance secrète, les procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation, la communication et la destruction des données interceptées, les procédures d'autorisation, les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne »[178] [179]. Dans les affaires évoquées ci-dessus, la Cour a condamné la Hongrie et le Royaume-Uni pour non-respect de ces conditions. Quant à la Suède, la Cour ne l'a pas condamnée car elle a considéré que le système suédois offrait des garanties adéquates et suffisantes contre l'arbitraire et le risque d'abus.

Il y a un certain paradoxe à confronter cette approche exigeante de la Cour européenne des droits de l'homme ainsi que la condamnation de la Cour de justice de l'UE au nom du caractère disproportionné de l'obligation de conservation systématique et massive des données de trafic et de localisation, avec la pratique actuelle des acteurs privés de messagerie tels Messenger, Instagram, WhatsApp, Wechat ou Skype. Ces derniers conservent les messages échangés – tant les données de

175 Cour eur. D.H. (Gde ch.), 12 janvier 2016, *Szabo et Vissy c. Hongrie*. Voy. F. DUBUISSON, « La Cour européenne des droits de l'homme et la surveillance de masse », *op. cit.*, pp. 876 et s.

176 Cour eur. D.H., 19 juin 2018, *Centrum for Rädvisa c. Suède*.

177 Cour eur. D.H., 13 septembre 2018, *Big Brother Watch and Others c. Royaume-Uni*.

178 Cour eur. D.H., 4 décembre 2015, *Roman Zakharov c. Russie*, § 238.

179 « Dans sa jurisprudence relative aux mesures de surveillance secrète, la Cour énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements », Cour eur. D.H., *Roman Zakharov c. Russie*, préc., § 231 ; *Centrum for Rädvisa c. Suède*, préc., § 103.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



communication que le contenu [180] – et les traces de toute activité recourant à leurs services [181]. Les informations recueillies par ces acteurs leur servent à réaliser et alimenter le profilage de leurs clients et des personnes en lien avec ceux-ci. L'exploitation commerciale des profils très fins obtenus et sans cesse actualisés est la base de la rentabilité économique des services offerts gratuitement. Même si elle est acceptée socialement au nom d'un pragmatisme économe, cette capacité de surveillance totale des échanges par les acteurs privés concernés ne manque pas de susciter la réflexion sur la société qu'on est en train d'ériger. L'inquiétude s'accentue lorsqu'on prend aussi en considération le partage des données ainsi recueillies avec des tiers, acteurs du secteur public ou privé. Enfin, il est à noter que le profilage, qui servait surtout initialement à orienter les opérations de marketing et réduisait les personnes concernées à leur dimension de consommateurs, a désormais également un impact politique et porte atteinte au droit à l'information. Comme évoqué plus haut, la pratique a montré que le profilage peut conduire à sélectionner les informations véhiculées jusqu'aux personnes concernées et avoir une influence manifeste et préoccupante sur des campagnes électorales et lors de référendums.

### C. – *Surveillance des communications professionnelles*

La protection contre la surveillance des individus à travers leurs communications s'étend au lieu du travail [182]. C'est principalement la protection contre les agissements de l'employeur qui est ici en cause. Il est désormais loin le temps où l'on disait que la vie privée s'arrêtait à la porte de l'entreprise ou du bureau. Considéré avec sa casquette d'employé ou de salarié, l'individu jouit de la même protection que contre les opérations de surveillance réalisées par les autorités publiques. Ce droit à

180 WhatsApp signale toutefois que s'ils conservent bien une série de données entourant l'utilisation de leurs services, ils ne conservent normalement pas les messages échangés. Ceux-ci sont stockés sur les terminaux des utilisateurs : « Nous ne conservons pas vos messages durant la prestation de nos Services en temps normal. Une fois que vos messages (y compris vos discussions, photos, vidéos, messages vocaux, fichiers et informations de partage de la position) sont transmis, ils sont supprimés de nos serveurs. Vos messages sont stockés dans votre propre appareil. Si un message ne peut pas être transmis immédiatement (par exemple si vous êtes hors ligne), nous le conservons sur nos serveurs pendant 30 jours au maximum pour essayer de le transmettre. Si un message n'est toujours pas transmis après 30 jours, nous le supprimons » (https://www.whatsapp.com/legal/#privacy-policy-information-we-collect).

181 Voy. par exemple la « Politique d'utilisation des données » de Facebook, à l'adresse https://www.facebook.com/policy.php et la « Politique de confidentialité » d'Instagram à l'adresse https://help.instagram.com/155833707900388.

182 Voy. pour une analyse approfondie de la surveillance sur le lieu de travail, la contribution de Karen Rosier dans le présent ouvrage.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



la protection de la vie privée dans les relations de travail et sur le lieu de travail a été énoncé à plusieurs reprises par la Cour européenne des droits de l'homme[183]. L'arrêt *Barbulescu* prononcé en Grande chambre[184] l'a mis remarquablement en lumière, en en dessinant précisément les contours. Ainsi, la Cour a établi les critères à appliquer pour apprécier la légalité ou non d'une mesure de surveillance par l'employeur de la correspondance électronique des salariés. Ces critères portent sur l'information préalable des travailleurs quant à l'existence et à la nature de la surveillance, sur l'étendue de la surveillance effectuée (accès aux contenus ou aux seules données de communication), sur la justification des mesures de surveillance, sur la possibilité de mesures alternatives moins attentatoires, sur les conséquences de la surveillance pour l'employé et sur l'existence de garanties adéquates au bénéfice de celui-ci[185].

## VIII. Conclusion

Depuis plusieurs décennies, le Conseil de l'Europe et l'Union européenne sont les fers de lance de la protection des données à caractère personnel. L'année 2018 aura marqué un tournant décisif dans leur action, chacune de ces organisations ayant vu un texte porteur d'un régime de protection des données radicalement modernisé adopté ou entré en application. Cet *aggiornamento* législatif vise à ajuster la protection des individus en tenant compte des bouleversements technologiques, économiques, sociaux et culturels induits notamment par le déploiement d'Internet.

Tant la Convention 108+ que le RGPD exercent désormais une influence bien au-delà des frontières européennes[186]. Appliqués dans le contexte d'Internet, ces textes promettent d'œuvrer au rééquilibrage des rapports entre l'individu, les acteurs économiques et les autorités publiques, tout en contrant l'opacité ambiante et la puissance des outils techniques.

La Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne ont démontré, ces dernières années tout particulièrement, qu'elles tenaient à jouer un rôle prépondérant dans l'édification

183 Voy. par exemple Cour eur. D.H., 28 novembre 2017, *Antovic et Mirkovic c. Montenegro*.
184 Cour eur. D.H. (Gde ch.), 5 septembre 2017, *Barbulescu c. Roumanie*.
185 *Ibid.*, §§ 121 et 122.
186 Voy. également la contribution de Claire Gayrel dans le présent ouvrage.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019

strada lex



d'une société numérique répondant aux exigences de la démocratie et de l'état de droit. La reconnaissance par la Cour européenne des droits de l'homme du droit à l'auto-détermination informationnelle en tant que partie intégrante du droit à la vie privée, la condamnation par la Cour de justice de la surveillance de masse des communications électroniques, et le soin scrupuleux avec lequel ces deux juridictions veillent au respect du principe de proportionnalité lors du traitement de données à caractère personnel, sont autant de preuve de leur engagement, allant parfois jusqu'à l'audace, pour tracer les contours et appliquer les règles de protection des données dans l'univers connecté d'aujourd'hui.



virginie.marot@unamur.be
Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel
Éditions Larcier - © Larcier - 29/05/2019